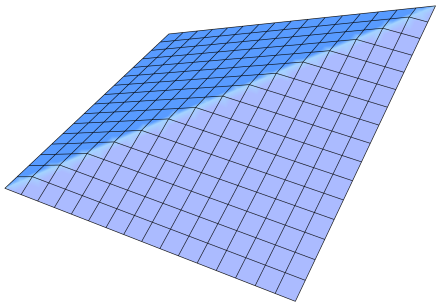


PMATH 340: Elementary Number Theory

Prof. Wentang Kuo • Fall 2015 • University of Waterloo
MWF 11:30AM–12:20PM in B2 350

Transcribed, LaTeXed, and edited by Rob Zimmerman

Note: These are personal lecture notes, not official course materials. They may contain errors (which by default you should attribute to me, Rob Zimmerman, rather than the course instructor). The permanent home of these — and all of my other lecture notes — is https://rob-zimmerman.github.io/coursenotes.

Contents

Lecture 1 — Monday, September 14, 2015

1. Diophantine Equations and Arithmetic Functions

Linear Diophantine Equations

Our first examples show that the ambient set matters when solving a Diophantine equation.

Example 1.1 Solve $2x = 3$ over $\mathbb{R}$.

Solution. Dividing by 2 gives $x = 3/2$. □

Example 1.2 Solve $2x = 3$ for $x \in \mathbb{Z}$.

Solution. Dividing by 2 gives $x = 3/2 \notin \mathbb{Z}$, so there are no integer solutions. □

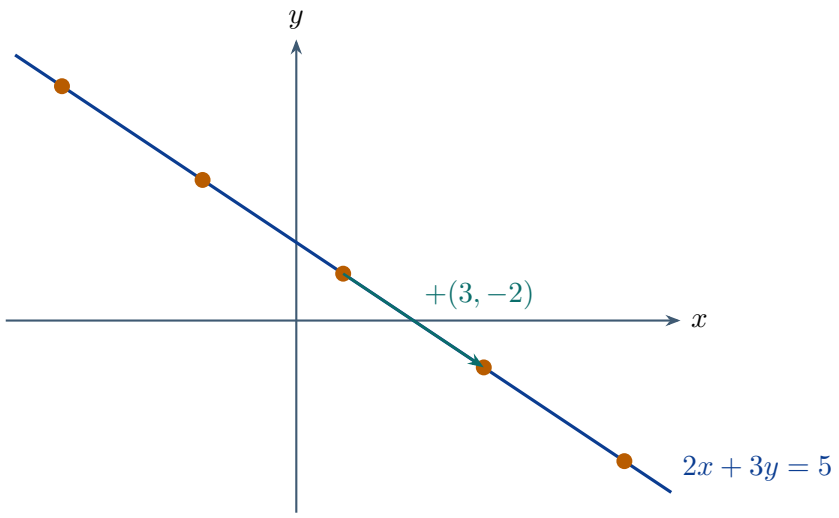
Example 1.3 Solve $2x + 3y = 5$ for $x, y \in \mathbb{Z}$.

Solution. The integer solutions are

$$\begin{cases} x = 1 + 3n \\ y = 1 - 2n \end{cases} \quad \text{for } n \in \mathbb{Z}.$$

□

The real solutions form a line, but the integer solutions are the equally spaced lattice points marked in Figure 1. Moving from one integer solution to the next adds $(3, -2)$, which is the general homogeneous solution of $2x + 3y = 0$.



the Diophantine solutions are a one-dimensional lattice inside the real solution line

FIGURE 1

Definition 1.4 A triple (a, b, c) of integers is a **Pythagorean triple** if

$$a^2 + b^2 = c^2.$$

Over $\mathbb{R}$, finding such triples is easy: after choosing $a, b \in \mathbb{R}$, we may take $c = \pm\sqrt{a^2 + b^2}$. The number-theoretic problem is to find the triples for which $a, b, c \in \mathbb{Z}$.

Since $(-a)^2 = a^2$, we may assume that $a, b, c \in \mathbb{N}$. If $a = 0$ or $b = 0$, then the solution is trivial, so we exclude these cases. If a, b, c have a common divisor d, so that

$$a = a'd, \qquad b = b'd, \qquad \text{and} \qquad c = c'd$$

for some $a', b', c', d \in \mathbb{Z}$, then

$$\begin{aligned} a^2 + b^2 = c^2 &\iff a'^2d^2 + b'^2d^2 = c'^2d^2 \\ &\iff a'^2 + b'^2 = c'^2. \end{aligned}$$

Thus we may reduce to the case where a, b, c have no common divisor greater than 1.

Definition 1.5 A **primitive Pythagorean triple** is a Pythagorean triple (a, b, c) such that a, b, c have no common divisor greater than 1.

It remains to determine all primitive Pythagorean triples.

Example 1.6 Some primitive Pythagorean triples are

$$3^2 + 4^2 = 5^2, \qquad 5^2 + 12^2 = 13^2, \qquad 8^2 + 15^2 = 17^2, \qquad \text{and} \qquad 7^2 + 24^2 = 25^2.$$

These examples suggest a parity pattern.

Proposition 1.7 In a primitive Pythagorean triple $a^2 + b^2 = c^2$, the integer c is odd.

Proof. Suppose for a contradiction that c is even. Then $a^2 + b^2$ is even, so a and b have the same parity. They cannot both be even, since then a, b, c would have 2 as a common factor. Therefore both a and b are odd. Write

$$a = 2x + 1, \qquad b = 2y + 1, \qquad \text{and} \qquad c = 2z$$

for some $x, y, z \in \mathbb{Z}$. Then

$$\begin{aligned} (2x + 1)^2 + (2y + 1)^2 &= (2z)^2 \\ (4x^2 + 4x + 1) + (4y^2 + 4y + 1) &= 4z^2 \\ 4(x^2 + x + y^2 + y) + 2 &= 4z^2, \end{aligned}$$

which is impossible because the left-hand side is congruent to 2 modulo 4, while the right-hand side is divisible by 4. Hence c is odd. □

After possibly interchanging a and b, we may assume that a is odd and b is even. Then c is odd by Proposition 1.7, and

$$a^2 + b^2 = c^2 \iff a^2 = c^2 - b^2 = (c-b)(c+b).$$

For example,

$$3^2 = 5^2 - 4^2 = (5-4)(5+4) = 1 \cdot 9 = 1^2 \cdot 3^2.$$
$$5^2 = 13^2 - 12^2 = \cdots = 1^2 \cdot 5^2.$$
$$15^2 = 17^2 - 8^2 = (17+8)(17-8) = 25 \cdot 9 = 5^2 \cdot 3^2.$$

Proposition 1.8 If a is odd in a primitive Pythagorean triple $a^2 + b^2 = c^2$, then $c - b$ and $c + b$ are squares.

Lecture 2 — Wednesday, September 16, 2015

Proof. Let p be a prime factor of a. Then

$$p^2 \mid a^2 = (c-b)(c+b).$$

Since a is odd, p is odd. We claim that p cannot divide both $c-b$ and $c+b$. Indeed, if it did, then

$$p \mid (c-b) + (c+b) = 2c \qquad \text{and} \qquad p \mid (c+b) - (c-b) = 2b.$$

Since p is odd, this implies $p \mid c$ and $p \mid b$. But $p \mid a$ as well, contradicting primitivity. Thus no prime factor of a can occur in both $c-b$ and $c+b$.

By the unique factorization of integers, the prime factors appearing in $c-b$ and $c+b$ therefore split the even exponents in the factorization of a^2. Hence both $c-b$ and $c+b$ are squares. □

Let $c + b = s^2$ and $c - b = t^2$. Then $a = st$, and

$$c + b = s^2 \qquad \text{and} \qquad c - b = t^2$$

imply

$$c = \frac{s^2 + t^2}{2} \qquad \text{and} \qquad b = \frac{s^2 - t^2}{2}.$$

Conversely, these formulas produce a Pythagorean triple:

$$a^2 + b^2 = (st)^2 + \left(\frac{s^2 - t^2}{2}\right)^2 = s^2t^2 + \frac{s^4 - 2s^2t^2 + t^4}{4} = \frac{s^4 + 2s^2t^2 + t^4}{4} = \left(\frac{s^2 + t^2}{2}\right)^2 = c^2.$$

Remark 2.1 For (a, b, c) to be primitive, the integers s and t must be coprime and both must be odd. The converse is also true.

Theorem 2.2 Let a, b, c be positive integers with a odd and b even. Then (a, b, c) is a primitive Pythagorean triple if and only if there exist odd coprime positive integers $s > t$ such that

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad c = \frac{s^2 + t^2}{2}.$$

Proof. *Forward implication.* Suppose that (a, b, c) is a primitive Pythagorean triple with a odd and b even. By Proposition 1.8, there are positive integers $s > t$ such that

$$c + b = s^2 \qquad \text{and} \qquad c - b = t^2.$$

Then $a^2 = (c - b)(c + b) = s^2t^2$, so $a = st$. Adding and subtracting the equations for $c + b$ and $c - b$ gives the desired formulas for b and c. Since $c + b$ and $c - b$ are odd, both s and t are odd. If a prime divided both s and t, then it would divide $a = st$, $b = (s^2 - t^2)/2$, and $c = (s^2 + t^2)/2$, contradicting primitivity. Thus s and t are coprime.

Reverse implication. Suppose that $s > t$ are odd coprime positive integers and define a, b, c by the displayed formulas. Since s and t are odd, b and c are integers. The computation above shows that $a^2 + b^2 = c^2$. It remains to check primitivity. The integer $a = st$ is odd, and $c = (s^2 + t^2)/2$ is also odd, so 2 is not a common divisor of a, b, c. If an odd prime p divided all three of a, b, c, then $p \mid st$, so p divides s or t. Since p also divides both b and c, it divides $b + c = s^2$ and $c - b = t^2$, hence it divides both s and t, contradicting $\gcd(s, t) = 1$. Therefore the triple is primitive. □

Euler's Theorem

Theorem 2.3 Let a, b, c and m be integers and suppose that $\gcd(c, m) = 1$ and $ac \equiv bc \pmod{m}$. Then $a \equiv b \pmod{m}$.

Proof. By Bezout's identity, there are integers u, v such that $uc + vm = 1$. The congruence $ac \equiv bc \pmod{m}$ says that $m \mid c(a - b)$. Multiplying the Bezout identity by $a - b$ gives

$$a - b = uc(a - b) + vm(a - b).$$

Both terms on the right are divisible by m, so $m \mid a - b$. Hence $a \equiv b \pmod{m}$. □

Theorem 2.4 (Fermat's little theorem) Let p be a prime and $\gcd(a, p) = 1$ with $a \in \mathbb{Z}$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. If p is prime and $(a, p) = 1$, then the residues

$$1, 2, 3, \ldots, p - 1$$

are the same as

$$a, 2a, 3a, \ldots, a(p - 1) \pmod{p},$$

possibly in a different order. For instance, when $a = 2$ and $p = 5$, multiplication by 2 sends

$$1, 2, 3, 4 \longmapsto 2, 4, 1, 3 \pmod{5}.$$

Therefore

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p - 1) &\equiv (a \cdot 1)(a \cdot 2) \ldots (a \cdot (p - 1)) \pmod{p} \\ &\equiv a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p - 1) \pmod{p}. \end{aligned}$$

Cancelling the product $1 \cdot 2 \cdot \cdots \cdot (p - 1)$ gives $a^{p-1} \equiv 1 \pmod{p}$. □

Question 2.5 The natural analogue of Theorem 2.4 asks whether, for integers a and m

with $(a, m) = 1$, there is a useful exponent $\phi(m)$ such that

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

For a prime p, Theorem 2.4 says that $\phi(p) = p - 1$ works.

Lecture 3 — Friday, September 18, 2015

For a general modulus m, the analogue of the nonzero residues modulo a prime is the reduced residue system.

Definition 3.1 For $m \geq 1$, define

$$R_m = \{n \in \mathbb{Z} : 1 \leq n \leq m,\ (n, m) = 1\},$$

the set of all integers between 1 and m that are coprime to m. The number $\phi(m) = |R_m|$ is called **Euler's totient function**.

Example 3.2 $R_{12} = \{1, 5, 7, 11\}$. If $a = 5$, then

$$\{1, 5, 7, 11\} \pmod{12} = \{5, 25, 35, 55\} \pmod{12} = \{5, 1, 11, 7\}.$$

As in the proof of Fermat's little theorem,

$$\begin{aligned} 1 \cdot 5 \cdot 7 \cdot 11 &\equiv (5 \cdot 1)(5 \cdot 5)(5 \cdot 7)(5 \cdot 11) \pmod{12} \\ &\equiv 5^4(1 \cdot 5 \cdot 7 \cdot 11) \pmod{12}, \end{aligned}$$

so $5^4 \equiv 1 \pmod{12}$. Here $\phi(12) = 4$.

Multiplication by a unit merely permutes the reduced residue system. For $a = 5$ modulo 12, that permutation is displayed in Figure 2; because no residue is lost or repeated, the products of the two rows agree modulo 12.

Theorem 3.3 (Euler's theorem) Let $a, m \in \mathbb{Z}$ with $m \geq 2$ and $(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

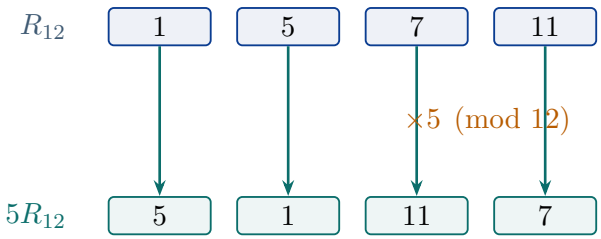


FIGURE 2

Proof. Write $R_m = \{r_1, r_2, \ldots, r_{\phi(m)}\}$. We first show that

$$\{ar_1, \ldots, ar_{\phi(m)}\} \pmod{m}$$

is the same set as R_m, possibly in a different order.

We need two facts:

1. Each ar_i is coprime to m.
2. The residues ar_i are distinct modulo m.

For (1), since $(a, m) = 1$ and $(r_i, m) = 1$, we have $(ar_i, m) = 1$.

For (2), suppose that

$$ar_i \equiv ar_j \pmod{m}.$$

By Theorem 2.3, $r_i \equiv r_j \pmod{m}$. Since r_i and r_j are the chosen representatives in R_m, this implies $r_i = r_j$, and hence $i = j$.

Thus multiplication by a permutes the reduced residue system modulo m. Therefore

$$\begin{aligned} r_1 \ldots r_{\phi(m)} &\equiv (ar_1) \ldots (ar_{\phi(m)}) \pmod{m} \\ &\equiv a^{\phi(m)} r_1 \ldots r_{\phi(m)} \pmod{m}. \end{aligned}$$

The product $r_1 \ldots r_{\phi(m)}$ is coprime to m, so another application of cancellation gives $a^{\phi(m)} \equiv 1 \pmod{m}$. □

To use Theorem 3.3, we need a way to compute $\phi(m)$.

Example 3.4 Since 3 is prime, $\phi(3) = 3 - 1 = 2$. Also $\phi(2) = 1$,

$$\phi(4) = 2 \qquad \text{because} \qquad R_4 = \{1, 3\},$$

and $\phi(6) = 2$ because $R_6 = \{1, 5\}$. Finally,

$$\phi(12) = 4 = 2 \cdot 2 = 2^2.$$

Could ϕ be multiplicative?

Proposition 3.5 Let m, n be positive integers with $mn \geq 2$. If $(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Assuming Proposition 3.5, if

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

is the prime factorization of m, then

$$\phi(m) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k}).$$

Thus it remains to compute $\phi(p^\alpha)$ for prime powers.

Theorem 3.6 Let p be prime and let $\alpha \geq 1$. Then $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Lecture 4 — Monday, September 21, 2015

Recall that $\phi(m) = |R_m|$, where

$$R_m = \{n \in \mathbb{Z} : 1 \leq n \leq m,\ (n, m) = 1\},$$

and that Theorem 3.3 states that $a^{\phi(m)} \equiv 1 \pmod{m}$ whenever $(a, m) = 1$.

Proof of Theorem 3.6. The integers between 1 and p^α which are not coprime to p^α are precisely the multiples of p:

$$\{p, 2p, \dots, p^{\alpha-1}p\}.$$

There are $p^{\alpha-1}$ such multiples. Therefore

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

□

Proof of Proposition 3.5. Let m and n be positive integers with $(m,n)=1$. Consider the sets

$$B = \{b : 1 \le b \le mn,\ (b, mn) = 1\}$$

and

$$C = \{(c,d) : 1 \le c \le m,\ 1 \le d \le n,\ (c,m) = 1,\ (d,n) = 1\} = R_m \times R_n.$$

We construct a bijection from B to C. Given $b \in B$, let c and d be the unique representatives satisfying

$$1 \le c \le m, \qquad 1 \le d \le n, \qquad b \equiv c \pmod m, \qquad \text{and} \qquad b \equiv d \pmod n.$$

Define $f(b) = (c,d)$.

Example 4.1 If $m = 4$ and $n = 3$, then $mn = 12$ and

$$R_{12} = B = \{1, 5, 7, 11\}.$$

The map f is given by

$$f(1) = (1,1), \qquad f(5) = (1,2), \qquad f(7) = (3,1), \qquad \text{and} \qquad f(11) = (3,2).$$

Thus

$$C = R_m \times R_n = \{1,3\} \times \{1,2\} = \{(1,1),(1,2),(3,1),(3,2)\} = \{f(1), f(5), f(7), f(11)\}.$$

It remains to show that f is a bijection.

1. The map f is injective. Indeed, if $f(b) = f(b') = (c,d)$, then

   $$b \equiv b' \equiv c \pmod m \qquad \text{and} \qquad b \equiv b' \equiv d \pmod n.$$

   By the Chinese remainder theorem, this system has a unique solution modulo mn, so $b = b'$ as representatives in $\{1, \dots, mn\}$.

2. The map f is surjective. Given $(c,d) \in R_m \times R_n$, the Chinese remainder theorem gives a

solution b modulo mn to

$$b \equiv c \pmod{m} \qquad \text{and} \qquad b \equiv d \pmod{n}.$$

Since $(c, m) = 1$, $(d, n) = 1$, and $(m, n) = 1$, this representative satisfies $(b, mn) = 1$, so $b \in B$ and $f(b) = (c, d)$.

Therefore

$$\phi(mn) = |B| = |C| = |R_m \times R_n| = |R_m|\,|R_n| = \phi(m)\phi(n).$$

□

Theorem 4.2 Let $m \geq 2$ be an integer, and write

$$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

for its prime factorization. Then

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Proof. By Proposition 3.5 and Theorem 3.6,

$$\begin{aligned}
\phi(m) &= \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) \\
&= m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

□

Lecture 5 — Wednesday, September 23, 2015

Question 5.1 How do we solve congruences of the form

$$x^k \equiv b \pmod{m}?$$

Euler's theorem might help in certain cases.

Example 5.2 Solve $x^{25} \equiv 7 \pmod{135}$.

Solution. Any solution x must be coprime to 135, since $\gcd(x, 135)$ divides $\gcd(7, 135) = 1$. We have $\phi(135) = 72$, and $(25, 72) = 1$. Choose integers $u = 49$ and $v = 17$ satisfying

$$25u - 72v = 1.$$

Then Euler's theorem gives $x^{72} \equiv 1 \pmod{135}$, so

$$x = x^{25u-72v} = (x^{25})^u (x^{72})^{-v} \equiv 7^{49} \equiv 52 \pmod{135}.$$

Thus the unique solution is $x \equiv 52 \pmod{135}$. □

More generally, let $b, k, m \in \mathbb{Z}$ with $k, m \in \mathbb{N}$, $(b, m) = 1$, and $(k, \phi(m)) = 1$. To solve $x^k \equiv b \pmod{m}$, we may do the following:

1. Compute $\phi(m)$.
2. Use the extended Euclidean algorithm to find integers u, v such that $ku - \phi(m)v = 1$.
3. Compute $b^u \pmod{m}$.

This gives the unique solution modulo m.

Remark 5.3 If $f(x)$ is a polynomial, the number of solutions to $f(x) \equiv 0 \pmod{m}$ does not necessarily match the degree of $f(x)$.

Example 5.4 The polynomial congruence

$$x(x-1)(x-2) \equiv 0 \pmod{6}$$

has six solutions modulo 6, even though the polynomial has degree 3.

Sums of Divisors

Question 5.5 For $n \in \mathbb{N}$, define

$$F(n) = \sum_{d|n} \phi(d),$$

where the sum is taken over the positive divisors of n. What is $F(n)$?

Example 5.6 If $p \in \mathbb{P}$, then the positive divisors of p are 1 and p, so

$$F(p) = \phi(1) + \phi(p) = 1 + (p-1) = p.$$

Example 5.7 If $n = p^k$ for a prime p, then the positive divisors are $1, p, p^2, \ldots, p^k$, and

$$F(p^k) = \sum_{j=0}^{k} \phi(p^j) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k.$$

Example 5.8 The positive divisors of 15 are $1, 3, 5, 15$, so

$$F(15) = \phi(1) + \phi(3) + \phi(5) + \phi(15) = 1 + 2 + 4 + 8 = 15.$$

Could it be that $F(n) = n$ for all $n \in \mathbb{N}$?

Theorem 5.9 For every $n \in \mathbb{N}$,

$$\sum_{d|n} \phi(d) = n.$$

Proof. First suppose that $(m,n)=1$. Let $d_1,\dots,d_k$ be the positive divisors of m, and let $e_1,\dots,e_\ell$ be the positive divisors of n. Since $(m,n)=1$, we have $(d_i,e_j)=1$ for each i and j, and the positive divisors of mn are precisely the products d_ie_j. Hence

$$\begin{aligned} F(mn) &= \sum_{i=1}^{k}\sum_{j=1}^{\ell}\phi(d_ie_j) \\ &= \sum_{i=1}^{k}\sum_{j=1}^{\ell}\phi(d_i)\phi(e_j) \\ &= \left(\sum_{i=1}^{k}\phi(d_i)\right)\left(\sum_{j=1}^{\ell}\phi(e_j)\right) \\ &= F(m)F(n). \end{aligned}$$

Now write $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$. By multiplicativity of F on coprime inputs and the computation for prime powers above,

$$F(n)=F(p_1^{\alpha_1})\dots F(p_k^{\alpha_k})=p_1^{\alpha_1}\dots p_k^{\alpha_k}=n.$$

□

Lecture 6 — Friday, September 25, 2015

Example 6.1 Take $m=14$ and $n=15$. Their positive divisors are

$$d_1,d_2,d_3,d_4=1,2,7,14 \qquad \text{and} \qquad e_1,e_2,e_3,e_4=1,3,5,15.$$

Because $(14,15)=1$, every positive divisor of 210 is uniquely a product d_ie_j. Therefore

$$\begin{aligned} F(210) &= \sum_{i=1}^{4}\sum_{j=1}^{4}\phi(d_ie_j) \\ &= \sum_{i=1}^{4}\sum_{j=1}^{4}\phi(d_i)\phi(e_j) \end{aligned}$$

$$
\begin{aligned}
&= 1 \cdot \left(\sum_{j=1}^{4} \phi(e_j) \right) + 1 \cdot \left(\sum_{j=1}^{4} \phi(e_j) \right) + 6 \cdot \left(\sum_{j=1}^{4} \phi(e_j) \right) + 6 \cdot \left(\sum_{j=1}^{4} \phi(e_j) \right) \\
&= 14 \cdot (1 + 2 + 4 + 8) \\
&= 14 \cdot 15 \\
&= 210.
\end{aligned}
$$

The 4×4 array in Figure 3 makes the multiplicative step concrete: every divisor of $210 = 14 \cdot 15$ occurs exactly once as a row divisor of 14 times a column divisor of 15.

$e \mid 15$

$d \mid 14$

	1	3	5	15
1	1	3	5	15
2	2	6	10	30
7	7	21	35	105
14	14	42	70	210

coprimality makes the factorization $de \mid mn$ unique coordinate by coordinate

FIGURE 3

2. Primitive Roots and Indices

Primitive Roots

Our goal now is to understand the multiplicative structure of R_p, the reduced residue system modulo a prime p. All residue classes modulo p form a cyclic group under addition, generated by 1, but the nonzero classes represented by R_p form a group under multiplication. Is that group also generated by a single element? We don't know. We are a blind rat in a maze.

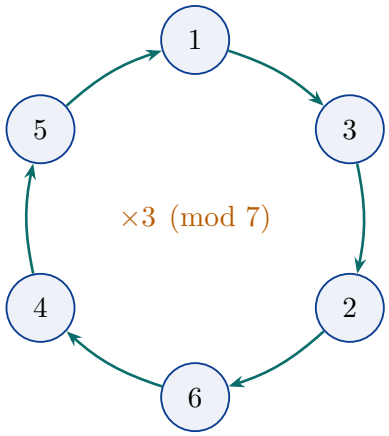
Question 6.2 By Fermat's little theorem, $k = p - 1$ satisfies $a^k \equiv 1 \pmod{p}$ for every a with $(a, p) = 1$. Is this the smallest exponent that works for all such a?

Example 6.3 For $p = 7$ and $a = 3$,

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad \text{and} \quad 3^6 \equiv 1 \pmod 7.$$

Thus 3 has exponent $6 = p - 1$ modulo 7.

The successive powers form the cycle in Figure 4. Starting at 1 and multiplying repeatedly by 3 visits every nonzero residue modulo 7 before returning to 1, so 3 is a primitive root.



a primitive root generates the entire multiplicative group in one cycle

FIGURE 4

Example 6.4 For $p = 11$ and $a = 2$,

i	1	2	3	4	5	6	7	8	9	10
$2^i \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Thus 2 has exponent $10 = p - 1$ modulo 11.

Theorem 6.5 (Primitive root theorem) Every prime has a primitive root. Equivalently, for every prime p, the smallest positive integer k such that $a^k \equiv 1 \pmod p$ for all $(a, p) = 1$ is $k = p - 1$.

Definition 6.6 Let $a, m \in \mathbb{Z}$ with $(a, m) = 1$. The smallest positive exponent e such that

$$a^e \equiv 1 \pmod m$$

is called the **exponent** of a modulo m, and is denoted $e_m(a)$. If $m = p$ is prime and $e_p(a) = p - 1$, then a is called a **primitive root** modulo p.

Proposition 6.7 Let $(a, m) = 1$ and $e_m(a) = e$. Then

$$a^1, a^2, \ldots, a^e$$

are all distinct modulo m. In particular, if a is a primitive root modulo p, then

$$\{a^1, a^2, \ldots, a^{p-1}\} \pmod{p}$$

is the full set of nonzero residue classes modulo p.

Proof. Suppose that

$$1 \leq i < j \leq e$$

and $a^j \equiv a^i \pmod{m}$. Since $(a, m) = 1$, cancellation gives

$$a^{j-i} \equiv 1 \pmod{m}.$$

But $0 < j - i < e$, contradicting the definition of $e = e_m(a)$. □

Lecture 7 — Monday, September 28, 2015

Recall that $e_m(a)$ denotes the exponent of a modulo m, and that a is a primitive root modulo a prime p when $e_p(a) = p - 1$. The primitive root theorem, Theorem 6.5, says that every prime has a primitive root.

Proposition 6.7 says that if $e = e_m(a)$, then $a^1, a^2, \ldots, a^e$ are all distinct modulo m.

Example 7.1 Modulo 7, the exponents of the nonzero residue classes are

$$e_7(1) = 1, \quad e_7(2) = 3, \quad e_7(3) = 6,$$
$$e_7(4) = 3, \quad e_7(5) = 6, \quad \text{and} \quad e_7(6) = 2.$$

All of these exponents divide 6.

Example 7.2 Modulo 11, the exponents of the nonzero residue classes are

a	1	2	3	4	5	6	7	8	9	10
$e_{11}(a)$	1	10	5	5	10	10	10	10	5	2

All of these exponents divide 10.

Primitive roots, when they exist, are not unique. The examples also suggest the exponent divisibility property below, which is effectively an application of Lagrange's theorem for finite groups.

Proposition 7.3 (Exponent divisibility property) Let $a, m \in \mathbb{Z}$ with $(a, m) = 1$. If $a^n \equiv 1 \pmod{m}$, then $e_m(a) \mid n$. In particular, $e_m(a) \mid \phi(m)$.

Proof. Let $e = e_m(a)$. By the division algorithm, write $n = qe + r$ with $0 \leq r < e$. Then

$$a^n = (a^e)^q a^r \equiv a^r \pmod{m}.$$

Since $a^n \equiv 1 \pmod{m}$, we have $a^r \equiv 1 \pmod{m}$. By the minimality of e, this forces $r = 0$. Hence $e \mid n$.

Taking $n = \phi(m)$ in Euler's theorem gives $e_m(a) \mid \phi(m)$. □

Example 7.4 Prove that 2 is a primitive root modulo 11.

Solution. By Proposition 7.3, the exponent $e_{11}(2)$ divides $\phi(11) = 10$. It is enough to check the proper divisors $1, 2, 5$:

$$2^1 \equiv 2, \qquad 2^2 \equiv 4, \qquad \text{and} \qquad 2^5 \equiv 32 \equiv 10 \pmod{11}.$$

None of these is congruent to 1 modulo 11, so $e_{11}(2) = 10$. Hence 2 is a primitive root modulo 11. □

Definition 7.5 Let $p \in \mathbb{P}$, and suppose $n \mid p-1$. Define

$$\Psi(n) = \#\{a : 1 \leq a \leq p-1,\ e_p(a) = n\}.$$

To prove Theorem 6.5, it is enough to show that $\Psi(p-1) \neq 0$.

Example 7.6 For $p = 7$, we have $\phi(7) = 6 = 2 \cdot 3$, and

$$\Psi(1) = 1, \qquad \Psi(2) = 1, \qquad \Psi(3) = 2, \qquad \text{and} \qquad \Psi(6) = 2.$$

Example 7.7 For $p = 11$, we have $\phi(11) = 10 = 2 \cdot 5$, and

$$\Psi(1) = 1, \qquad \Psi(2) = 1, \qquad \Psi(5) = 4, \qquad \text{and} \qquad \Psi(10) = 4.$$

Since every nonzero residue modulo p has some exponent dividing $p-1$, we have

$$\sum_{d \mid (p-1)} \Psi(d) = p - 1.$$

This resembles the identity

$$\sum_{d \mid n} \phi(d) = n$$

from Theorem 5.9.

Theorem 7.8 If p is prime and $n \mid p-1$, then

$$\Psi(n) = \phi(n).$$

Lecture 8 — Wednesday, September 30, 2015

We work towards a proof of Theorem 7.8. We know that

$$\sum_{d \mid (p-1)} \Psi(d) = p - 1.$$

Similarly, by Theorem 5.9,

$$\sum_{d|(p-1)} \phi(d) = p - 1.$$

If Theorem 7.8 is true, then $\Psi(p-1) = \phi(p-1) \geq 1$, so a primitive root exists. Thus Theorem 7.8 implies the primitive root theorem.

The definition of $\Psi(n)$ depends on p, but the proposed value $\phi(n)$ does not, provided that $n \mid p-1$. Directly counting the residue classes of exponent n is difficult. Instead, we count the solutions of $x^n \equiv 1 \pmod{p}$: if $e_p(a) = d$ and $d \mid n$, then $a^n \equiv 1 \pmod{p}$. This gives the following connection between $\Psi(n)$ and the nth roots of unity modulo p.

Lemma 8.1 Let p be prime. If $n \mid p-1$ and $d_1, \ldots, d_r$ are all the positive divisors of n, then

$$\sum_{d|n} \Psi(d) = \Psi(d_1) + \cdots + \Psi(d_r) = \#\{a : 1 \leq a \leq p-1,\ a^n \equiv 1 \pmod{p}\},$$

which is the number of solutions to the congruence $x^n \equiv 1 \pmod{p}$.

Proof. An integer a with $1 \leq a \leq p-1$ satisfies $a^n \equiv 1 \pmod{p}$ if and only if its exponent $e_p(a)$ divides n, by Proposition 7.3. Therefore the solutions are exactly the residue classes counted by $\Psi(d)$ as d ranges over the positive divisors of n. □

Proposition 8.2 Let p be prime, let $f(x) \in \mathbb{Z}[x]$, and suppose its reduction modulo p is a nonzero polynomial of degree n. Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions modulo p.

Proof. We argue by induction on n, working in the polynomial ring $\mathbb{F}_p[x]$. A nonzero constant polynomial has no roots. Now let $n \geq 1$. If f has no root, there is nothing to prove. Otherwise choose a root a. By the remainder theorem,

$$f(x) = (x - a)g(x)$$

in $\mathbb{F}_p[x]$, where g has degree $n-1$. If $b \neq a$ is another root of f, then

$$0 = f(b) = (b-a)g(b).$$

Since $\mathbb{F}_p$ is a field and $b - a \neq 0$, we have $g(b) = 0$. By the induction hypothesis, g has at most $n-1$ roots, so f has at most n roots. □

By Lemma 8.1 and Proposition 8.2, we have

$$\sum_{d|n} \Psi(d) = \#\{\text{solutions of } x^n \equiv 1 \pmod{p}\} \leq n.$$

We now prove the reverse inequality.

Lemma 8.3 If $n \mid p-1$, then the congruence

$$x^n \equiv 1 \pmod{p}$$

has exactly n solutions.

Proof. Write $p - 1 = nk$. Then

$$x^{p-1} - 1 = x^{nk} - 1 = (x^n - 1)(x^{n(k-1)} + x^{n(k-2)} + \cdots + x^n + 1).$$

By Fermat's little theorem, $x^{p-1} \equiv 1 \pmod{p}$ has the $p-1$ nonzero residue classes as solutions. The first factor $x^n - 1$ has at most n roots, and the second factor has degree $n(k-1)$ and hence at most $n(k-1)$ roots by Proposition 8.2. The two factors together must account for all $p - 1 = nk$ roots, so $x^n - 1$ has exactly n roots modulo p. □

Combining the previous lemmas gives, for every $n \mid p-1$,

$$\sum_{d|n} \Psi(d) = n.$$

Example 8.4 If $n = q$ is prime, then

$$\Psi(1) + \Psi(q) = q = \phi(1) + \phi(q).$$

Since $\Psi(1) = \phi(1) = 1$, we get $\Psi(q) = \phi(q) = q - 1$.

Example 8.5 If $n = qr$ with $q, r \in \mathbb{P}$, then

$$\sum_{d|qr} \Psi(d) = qr = \sum_{d|qr} \phi(d).$$

Since the equality has already been established for the proper divisors $1, q, r$, it follows that $\Psi(qr) = \phi(qr)$.

Lecture 9 — Friday, October 02, 2015

Recall that for $n \mid p - 1$,

$$\Psi(n) = \#\{a : 1 \leq a \leq p - 1,\ e_p(a) = n\},$$

and we have shown that

$$\sum_{d|n} \Psi(d) = n$$

while, by Theorem 5.9,

$$\sum_{d|n} \phi(d) = n.$$

We now prove Theorem 7.8.

Proof of Theorem 7.8. We use strong induction on the number of positive divisors of n. Let

$$1 = d_1, d_2, \ldots, d_k = n$$

be all positive divisors of n. The cases $k = 1$ and $k = 2$ follow directly from the displayed identities above.

Assume that the result is true for every positive integer with fewer than k positive divisors. By the identity already proved,

$$\Psi(d_1) + \Psi(d_2) + \cdots + \Psi(d_k) = n = \sum_{d|n} \phi(d) = \phi(d_1) + \cdots + \phi(d_k).$$

For $1 \leq j \leq k-1$, the divisor d_j is a proper divisor of n, so d_j has fewer positive divisors than n. By the induction hypothesis, $\Psi(d_j) = \phi(d_j)$ for $1 \leq j \leq k-1$. Therefore

$$\Psi(n) = \Psi(d_k) = n - (\Psi(d_1) + \cdots + \Psi(d_{k-1})) = n - (\phi(d_1) + \cdots + \phi(d_{k-1})) = \phi(n).$$

□

Example 9.1 For $n = 100 = 2^2 5^2$, the divisors are $2^\alpha 5^\beta$ with $0 \leq \alpha, \beta \leq 2$. If $d \mid n$ and $d < n$, then α and β cannot both be 2, so d has fewer divisors than n. This is the mechanism behind the induction argument.

Indices

By the primitive root theorem, for every prime p there exists $1 \leq g \leq p-1$ such that $e_p(g) = p-1$.

Corollary 9.2 Let $p \in \mathbb{P}$, and let g be a primitive root modulo p. Then

$$\{g^1, g^2, \ldots, g^{p-1}\} \pmod{p} = \{1, 2, 3, \ldots, p-1\}.$$

Proof. By Proposition 6.7, the powers $g^1, g^2, \ldots, g^{p-1}$ are all distinct modulo p. Since there are $p-1$ such powers, they must be congruent to the $p-1$ nonzero residue classes modulo p in some order. □

Example 9.3 For $p = 13$ and $g = 2$, the powers of 2 modulo 13 are:

i	1	2	3	4	5	6	7	8	9	10	11	12
$2^i \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

Definition 9.4 Let $p \in \mathbb{P}$, and let g be a primitive root modulo p. For $a \not\equiv 0 \pmod{p}$, the unique integer i with $1 \leq i \leq p-1$ and

$$a \equiv g^i \pmod{p}$$

is called the **index** of a modulo p for the base g, and is denoted $I_{p,g}(a)$.

The index plays the role of a discrete logarithm. As Figure 5 shows, it converts multiplication of

nonzero residue classes into addition of exponents modulo $p-1$.

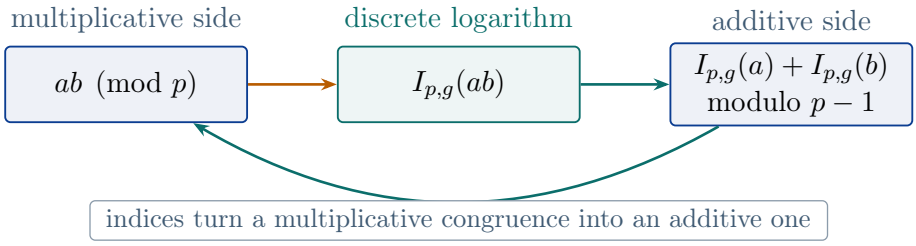


FIGURE 5

Example 9.5 For $p = 13$ and $g = 2$, the table in Example 9.3 gives

$$I_{13,2}(6) = 5 \qquad \text{and} \qquad I_{13,2}(12) = 6.$$

Theorem 9.6 (Index rules) Let $p \in \mathbb{P}$, and let g be a primitive root modulo p. Then the following hold:

1. $I(ab) \equiv I(a) + I(b) \pmod{p-1}$.
2. $I(a^k) \equiv kI(a) \pmod{p-1}$.

Proof. For (1), by definition,

$$a \equiv g^{I(a)} \pmod p \qquad \text{and} \qquad b \equiv g^{I(b)} \pmod p.$$

Thus

$$ab \equiv g^{I(a)+I(b)} \pmod p.$$

Since $g^{I(ab)} \equiv ab \pmod p$, we have

$$g^{I(ab)-I(a)-I(b)} \equiv 1 \pmod p.$$

By Proposition 7.3, $p-1 = e_p(g)$ divides $I(ab) - I(a) - I(b)$, so

$$I(ab) \equiv I(a) + I(b) \pmod{p-1}.$$

Lecture 10 — Monday, October 05, 2015

Proof continued. For (2), we compute

$$g^{I(a^k)} \equiv a^k \equiv \left(g^{I(a)}\right)^k \equiv g^{kI(a)} \pmod{p}.$$

Thus $g^{I(a^k)-kI(a)} \equiv 1 \pmod{p}$. Since g is a primitive root, $e_p(g) = p-1$, and Proposition 7.3 gives

$$(p-1) \mid \big(I(a^k) - kI(a)\big).$$

Therefore $I(a^k) \equiv kI(a) \pmod{p-1}$. □

Warning A common mistake is to reduce modulo p instead of modulo $p-1$. Don't do this!

Example 10.1 Let $p = 13$ and $g = 2$. Compute $12 \cdot 11 \pmod{13}$.

Solution. From the table in Example 9.3, $I(12) = 6$ and $I(11) = 7$. Hence

$$I(12 \cdot 11) \equiv I(12) + I(11) \equiv 6 + 7 \equiv 1 \pmod{12}.$$

Since $2^1 \equiv 2 \pmod{13}$, we get $12 \cdot 11 \equiv 2 \pmod{13}$. □

Example 10.2 Compute $11^{100} \pmod{13}$.

Solution. Using $I(11) = 7$,

$$I(11^{100}) \equiv 100I(11) \equiv 700 \equiv 4 \pmod{12}.$$

Since $2^4 \equiv 3 \pmod{13}$, we have $11^{100} \equiv 3 \pmod{13}$. □

Example 10.3 Solve $11x \equiv 2 \pmod{13}$.

Solution. Taking indices gives

$$I(11) + I(x) \equiv I(2) \pmod{12}.$$

Thus

$$7 + I(x) \equiv 1 \pmod{12},$$

so $I(x) \equiv 6 \pmod{12}$. Therefore $x \equiv 2^6 \equiv 12 \pmod{13}$. □

Example 10.4 Solve $3x^{21} \equiv 11 \pmod{13}$.

Solution. Taking indices gives

$$I(3) + 21I(x) \equiv I(11) \pmod{12}$$
$$4 + 21I(x) \equiv 7 \pmod{12}.$$

Thus $21I(x) \equiv 3 \pmod{12}$, or equivalently $7I(x) \equiv 1 \pmod{4}$. Hence

$$I(x) \equiv 3 \pmod{4},$$

so

$$I(x) \equiv 3, 7, 11 \pmod{12}.$$

Using the table for powers of 2 modulo 13, the solutions are

$$x \equiv 8, 11, 7 \pmod{13}.$$

□

Lecture 11 — Wednesday, October 07, 2015

3. Quadratic Residues and Reciprocity

Quadratic Residues and Legendre Symbols

Question 11.1 Given an integer a and a prime p, when does the congruence

$$x^2 \equiv a \pmod{p}$$

have a solution?

Over the integers, squares become sparse: among the integers from 1 to n, only about $\sqrt{n}$ of them are squares, and $\sqrt{n}/n \to 0$ as $n \to \infty$ (the proof does not require a PhD). Modulo a prime, the situation is very different.

Example 11.2 Modulo 2, both possible residue classes are squares, since

$$0^2 \equiv 0 \pmod{2} \qquad \text{and} \qquad 1^2 \equiv 1 \pmod{2}.$$

Modulo 11, the squares are displayed in the following table:

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1.

The symmetry comes from the identity $(p-b)^2 \equiv b^2 \pmod{p}$.

The five pairings in Figure 6 explain both the repeated entries in the table and the count $(p-1)/2$: the two inputs x and $p-x$ have the same nonzero square.

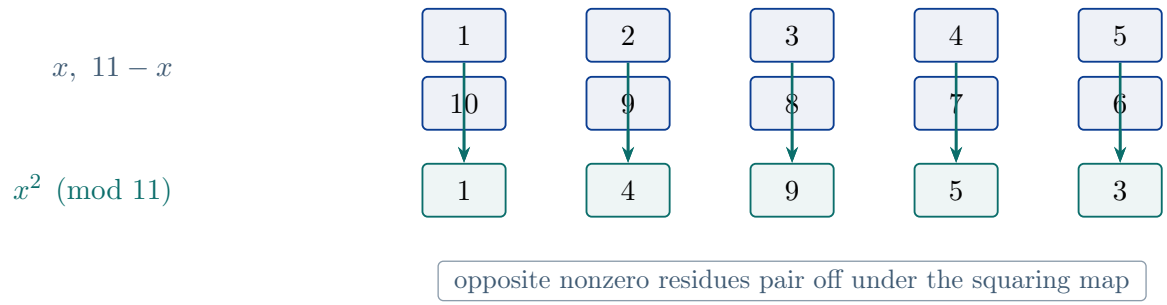


FIGURE 6

If p is odd and $x^2 \equiv a \pmod{p}$ has a solution, then $a \equiv i^2 \pmod{p}$ for some integer i with $0 \le i \le (p-1)/2$. Indeed, replacing i by $p-i$ gives the same square modulo p.

Definition 11.3 Let $p \in \mathbb{P}$, and let a be nonzero modulo p. We say that a is a **quadratic residue modulo p** if a is congruent to a square modulo p. Otherwise, a is a **quadratic nonresidue modulo p**.

Example 11.4 For $p = 11$, the quadratic residues are

$$1, 3, 4, 5, 9,$$

and the quadratic nonresidues are

$$2, 6, 7, 8, 10.$$

Proposition 11.5 Let p be an odd prime. There are exactly $(p-1)/2$ quadratic residues modulo p, and exactly $(p-1)/2$ quadratic nonresidues modulo p.

Proof. It is enough to show that the residue classes

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are distinct modulo p. Suppose that

$$1 \leq i \leq j \leq \frac{p-1}{2}$$

and that $i^2 \equiv j^2 \pmod{p}$. Then

$$p \mid (j^2 - i^2) = (j+i)(j-i).$$

Since p is prime, $p \mid j+i$ or $p \mid j-i$. The first possibility is impossible because

$$2 \leq i + j \leq p - 1.$$

For the second possibility, we have

$$0 \leq j - i \leq \frac{p-1}{2} - 1 < p,$$

so $p \mid j - i$ forces $j - i = 0$. Hence $i = j$, and therefore there are $(p-1)/2$ distinct quadratic residues. The remaining $(p-1)/2$ nonzero residue classes are quadratic nonresidues. □

Remark 11.6 Equivalently, if g is a primitive root modulo p, then a is a quadratic residue modulo p if and only if the index $I_{p,g}(a)$ is even. Indeed, by Corollary 9.2, every nonzero residue class is of the form g^j, and a square is therefore of the form g^{2j}.

Proposition 11.7 Let p be an odd prime, and let a_1, a_2 be nonzero modulo p.

1. If a_1 and a_2 are quadratic residues, then a_1a_2 is a quadratic residue.
2. If a_1 is a quadratic residue and a_2 is a quadratic nonresidue, then a_1a_2 is a quadratic nonresidue.
3. If a_1 and a_2 are quadratic nonresidues, then a_1a_2 is a quadratic residue.

Proof. For (1), write $a_1 \equiv b_1^2 \pmod{p}$ and $a_2 \equiv b_2^2 \pmod{p}$. Then

$$a_1a_2 \equiv (b_1b_2)^2 \pmod{p},$$

so a_1a_2 is a quadratic residue.

For (2), suppose for contradiction that a_1a_2 is a quadratic residue. Choose b_1 and b_3 such that

$$a_1 \equiv b_1^2 \pmod{p} \qquad \text{and} \qquad a_1a_2 \equiv b_3^2 \pmod{p}.$$

Since a_1 is nonzero modulo p, the class b_1 is invertible modulo p. Multiplying the second congruence by $(b_1^{-1})^2$ gives

$$a_2 \equiv (b_1^{-1}b_3)^2 \pmod{p},$$

contradicting that a_2 is a quadratic nonresidue.

Lecture 12 — Wednesday, October 14, 2015

Proof continued. For (3), let A be the set of quadratic residues and let B be the set of quadratic nonresidues. If $a_1 \in B$, then multiplication by a_1 gives a bijection of the nonzero residue classes modulo p. By (2), this bijection sends A into B. Since $|A| = |B|$ by Proposition 11.5, it sends A onto B. Hence the remaining set B must be sent onto A, so the product of two quadratic nonresidues is a quadratic residue. □

There is also a direct proof of (3) using indices.

Alternative proof of Proposition 11.7(3). Fix a primitive root g modulo p, and write $I(a) = I_{p,g}(a)$ for each nonzero residue class a modulo p. First observe that a is a quadratic residue modulo p exactly when $I(a)$ is even. Indeed, if $I(a) = 2s$, then

$$a \equiv g^{2s} \equiv (g^s)^2 \pmod{p},$$

so a is a quadratic residue. Conversely, suppose that $I(a) = 2s+1$. If a were a quadratic residue, then $a \equiv b^2 \pmod{p}$ for some nonzero residue class b. Since g is a primitive root modulo p, there is an integer i such that $b \equiv g^i \pmod{p}$. Thus

$$g^{2i} \equiv b^2 \equiv a \equiv g^{2s+1} \pmod{p}.$$

Since g has order $p-1$ modulo p, this gives

$$2i \equiv 2s+1 \pmod{p-1}.$$

This is impossible because $p-1$ is even, so congruent integers modulo $p-1$ have the same parity.

Now let a_1 and a_2 be quadratic nonresidues. Then $I(a_1)$ and $I(a_2)$ are odd, say

$$I(a_1) = 2i+1 \qquad \text{and} \qquad I(a_2) = 2j+1.$$

By Theorem 9.6,

$$I(a_1a_2) \equiv I(a_1) + I(a_2) \equiv 2(i+j+1) \pmod{p-1}.$$

Again, because $p-1$ is even, it follows that $I(a_1a_2)$ is even. Hence a_1a_2 is a quadratic residue. □

Definition 12.1 Let p be an odd prime, and let a be nonzero modulo p. The **Legendre symbol** of a modulo p is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Theorem 12.2 Let p be an odd prime, and let a, b be nonzero modulo p. Then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. This is exactly the three multiplication rules in Proposition 11.7, rewritten in the notation of Definition 12.1. □

To compute $\left(\frac{a}{p}\right)$, it is enough to factor a and compute the Legendre symbols of the prime factors of a.

Example 12.3 Using the table modulo 11 from Example 11.2, we have

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)(1) = -1.$$

Example 12.4 We have

$$\begin{aligned} \left(\frac{300}{13}\right) &= \left(\frac{2^2 \cdot 3 \cdot 5^2}{13}\right) \\ &= \left(\frac{2^2}{13}\right)\left(\frac{3}{13}\right)\left(\frac{5^2}{13}\right) \\ &= (\pm 1)^2 (1) (\pm 1)^2 \\ &= 1. \end{aligned}$$

Here $\left(\frac{3}{13}\right) = 1$ because $I_{13,2}(3) = 4$ is even.

Squares Modulo p

Question 12.5 What is $\left(\frac{-1}{p}\right)$?

For $p = 3$, the congruence $x^2 \equiv -1 \pmod 3$ has no solution, since

$$1^2 \equiv 1 \not\equiv -1 \pmod 3 \qquad \text{and} \qquad 2^2 \equiv 1 \not\equiv -1 \pmod 3.$$

Thus $\left(\frac{-1}{3}\right) = -1$. For $p = 5$, the congruence $x^2 \equiv -1 \pmod 5$ is equivalent to $x^2 \equiv 4 \pmod 5$, and $x = 2, 3$ are solutions. Thus $\left(\frac{-1}{5}\right) = 1$.

p	3	5	7	11	13	17	19	23	29	31
$x^2 \equiv -1 \pmod p$	none	$2, 3$	none	none	$5, 8$	$4, 13$	none	none	$12, 17$	none.

Is there a pattern here?

Lecture 13 — Friday, October 16, 2015

The previous table suggests that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

We will prove this using Euler's criterion.

Theorem 13.1 (Euler's criterion) Let p be an odd prime, and let a be nonzero modulo p. Then

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Proof. Let g be a primitive root modulo p. By the discussion after Proposition 11.5, the integer a is a quadratic residue modulo p if and only if $I_{p,g}(a)$ is even.

If a is a quadratic residue, write $a \equiv g^{2s} \pmod{p}$. Then

$$a^{(p-1)/2} \equiv (g^{2s})^{(p-1)/2} = (g^{p-1})^s \equiv 1 \pmod{p}.$$

This equals $\left(\frac{a}{p}\right)$.

If a is a quadratic nonresidue, write $a \equiv g^{2s+1} \pmod{p}$. Then

$$a^{(p-1)/2} \equiv g^{(2s+1)(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}.$$

By Fermat's little theorem,

$$\left(g^{(p-1)/2}\right)^2 \equiv 1 \pmod{p},$$

so $g^{(p-1)/2} \equiv \pm 1 \pmod{p}$. It cannot be congruent to 1, since otherwise $e_p(g)$ would be at most $(p-1)/2$, contradicting that g is a primitive root. Therefore

$$g^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

□

Theorem 13.2 (Quadratic reciprocity: part 1) Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Proof. By Theorem 13.1,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}.$$

Both sides are equal to either 1 or -1, so they are equal as integers. If $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is even; if $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd. □

Theorem 13.3 There are infinitely many primes congruent to 1 modulo 4.

Proof. Suppose, for contradiction, that $p_1, p_2, \ldots, p_r$ are all the primes congruent to 1 modulo 4.

Let

$$A = (2p_1p_2 \cdots p_r)^2 + 1.$$

Then $A \equiv 1 \pmod 4$, and no p_i divides A. Let q be a prime divisor of A. Since A is odd, q is odd. Also,

$$(2p_1p_2 \cdots p_r)^2 \equiv -1 \pmod q,$$

so -1 is a quadratic residue modulo q. By Theorem 13.2, this forces $q \equiv 1 \pmod 4$. This contradicts the assumption that all primes congruent to 1 modulo 4 were among the p_i, because none of the p_i divides A. □

Question 13.4 What is $\left(\frac{2}{p}\right)$?

Euler's criterion reduces this to computing $2^{(p-1)/2}$ modulo p. To find that, we need to build up $2^{(p-1)/2}$. We can do this by taking the set $\{1, 2, \ldots, p-1\}$ and multiplying by 2 to get the set $\{2, 4, \ldots, 2(p-1)\}$. Then $1 \cdot 2 \cdots (p-1) \equiv 2 \cdot 4 \cdots 2(p-1) \equiv 2^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod p$. Thus $1 \equiv 2^{p-1} \pmod p$. We have just reproved Fermat's little theorem for $a = 2$. Thus, to build up $2^{(p-1)/2}$, we consider the product

$$(2 \cdot 1)(2 \cdot 2) \cdots (2 \cdot \frac{p-1}{2}) = 2^{(p-1)/2} \cdot \left(1 \cdot 2 \cdots \frac{p-1}{2}\right).$$

Example 13.5 Let $p = 11$. Then

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 = 2^{(11-1)/2} \cdot 5!.$$

Reducing each factor to the interval $[-5, 5]$ gives

$$2, 4, 6, 8, 10 \equiv 2, 4, -5, -3, -1 \pmod{11}.$$

Thus

$$2^{(11-1)/2} \cdot 5! \equiv (-1)^3 \cdot 5! \pmod{11}.$$

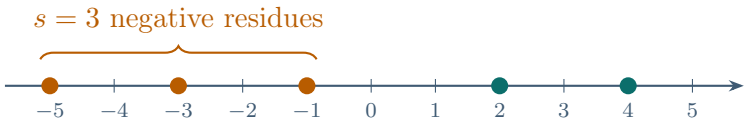
After cancelling 5!, we get

$$2^{(11-1)/2} \equiv -1 \pmod{11},$$

so Theorem 13.1 gives $\left(\frac{2}{11}\right) = -1$.

The centered residues in this calculation are shown on the number line in Figure 7. Exactly three

fall on the negative side, so Gauss's lemma returns the sign $(-1)^3 = -1$.



for $2, 4, 6, 8, 10$ modulo 11, the centered sign count determines $(2/11)$

FIGURE 7

Lecture 14 — Monday, October 19, 2015

Lemma 14.1 (Gauss's lemma) Let p be an odd prime, and let a be an integer with $\gcd(a, p) = 1$. For each integer i with $1 \leq i \leq (p-1)/2$, choose the unique integer u_i such that

$$ia \equiv u_i \pmod{p} \qquad \text{and} \qquad -\frac{p-1}{2} \leq u_i \leq \frac{p-1}{2}.$$

If s is the number of negative integers among the u_i, then

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Proof. We first claim that

$$\{|u_1|, |u_2|, \ldots, |u_{(p-1)/2}|\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}.$$

It is enough to show that these absolute values are distinct. Suppose that

$$1 \leq i < j \leq \frac{p-1}{2}$$

and $|u_i| = |u_j|$. If $u_i = u_j$, then

$$ia \equiv ja \pmod{p},$$

so $p \mid j - i$, which is impossible because $0 < j - i < p$. If $u_i = -u_j$, then

$$ia \equiv -ja \pmod{p},$$

so $p \mid i + j$, which is impossible because $2 \leq i + j \leq p - 1$. This proves the claim.

Multiplying the congruences $ia \equiv u_i \pmod{p}$ for $1 \leq i \leq (p-1)/2$ gives

$$\begin{aligned} a^{(p-1)/2}\left(\frac{p-1}{2}\right)! &\equiv u_1 u_2 \cdots u_{(p-1)/2} \pmod{p} \\ &\equiv (-1)^s |u_1||u_2| \cdots |u_{(p-1)/2}| \pmod{p} \\ &\equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

The factorial is invertible modulo p, so

$$a^{(p-1)/2} \equiv (-1)^s \pmod{p}.$$

The result now follows from Theorem 13.1. □

Computationally speaking, Gauss's lemma is much easier to use than Euler's criterion, because it replaces a large power computation by a sign count.

Example 14.2 Let $a = 2$. For $1 \leq i \leq (p-1)/2$, the integer $2i$ lies between 2 and $p-1$. It becomes negative after reduction to the interval $[-(p-1)/2, (p-1)/2]$ exactly when

$$2i > \frac{p}{2},$$

or equivalently when $i > p/4$. Hence the number of negative residues is

$$s = \frac{p-1}{2} - \left[\frac{p}{4}\right],$$

where $[x]$ is the greatest integer less than or equal to x (sometimes absurdly called the **Gauss symbol**).

Theorem 14.3 Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1, & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Equivalently,

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. By the preceding example and Lemma 14.1,

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/2-\left[\frac{p}{4}\right]}.$$

Thus it is sufficient to show that

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \pmod 2.$$

First suppose $p \equiv \pm 1 \pmod 8$. Write $p = 8k \pm 1$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned}\frac{p-1}{2} - \left[\frac{p}{4}\right] &= \frac{8k \pm 1 - 1}{2} - \left[\frac{8k \pm 1}{4}\right] \\ &= 4k + \frac{\pm 1 - 1}{2} - \left[2k \pm \frac{1}{4}\right] \\ &= \begin{cases} 4k - 2k = 2k, & \text{if } p = 8k+1, \\ 4k - 1 - (2k-1) = 2k, & \text{if } p = 8k-1, \end{cases}\end{aligned}$$

so the left-hand side is congruent to 0 modulo 2. Also,

$$\frac{p^2-1}{8} = \frac{64k^2 \pm 16k + 1 - 1}{8} = 8k^2 \pm 2k \equiv 0 \pmod 2.$$

Now suppose $p \equiv \pm 3 \pmod 8$. Write $p = 8k \pm 3$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned}\frac{p-1}{2} - \left[\frac{p}{4}\right] &= \frac{8k \pm 3 - 1}{2} - \left[\frac{8k \pm 3}{4}\right] \\ &= 4k + \frac{\pm 3 - 1}{2} - \left[2k \pm \frac{3}{4}\right] \\ &= \begin{cases} 4k + 1 - 2k = 2k + 1, & \text{if } p = 8k+3, \\ 4k - 2 - (2k-1) = 2k - 1, & \text{if } p = 8k-3, \end{cases}\end{aligned}$$

so the left-hand side is congruent to 1 modulo 2. On the other hand,

$$\frac{p^2-1}{8} = \frac{64k^2 \pm 48k + 9 - 1}{8} = 8k^2 \pm 6k + 1 \equiv 1 \pmod 2.$$

This completes the proof. □

Question 14.4 How do we compute $\left(\frac{q}{p}\right)$?

Lecture 15 — Wednesday, October 21, 2015

Quadratic Reciprocity and Jacobi Symbols

We already know the two supplementary laws for -1 and for 2:

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

We now turn to the general problem of computing $\left(\frac{q}{p}\right)$ for distinct odd primes p and q.

Example 15.1 We can reduce part of

$$\left(\frac{90}{101}\right)$$

using multiplicativity and the supplementary law for 2:

$$\begin{aligned}\left(\frac{90}{101}\right) &= \left(\frac{2 \cdot 3^2 \cdot 5}{101}\right) \\ &= \left(\frac{2}{101}\right)\left(\frac{3}{101}\right)^2\left(\frac{5}{101}\right) \\ &= (-1)(1)^2\left(\frac{5}{101}\right) \\ &= -\left(\frac{5}{101}\right).\end{aligned}$$

Thus the remaining issue is how to compare $\left(\frac{5}{101}\right)$ with $\left(\frac{101}{5}\right)$.

Remark 15.2 The squares modulo 5 are 1 and 4, so

$$\left(\frac{p}{5}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 4 \pmod 5, \\ -1, & \text{if } p \equiv 2, 3 \pmod 5. \end{cases}$$

Since $5 \equiv 1 \pmod 4$, the law below will imply that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ for odd primes $p \neq 5$.

Example 15.3 Compute $\left(\frac{5}{p}\right)$. It is easier to compute $\left(\frac{p}{5}\right)$:

$$\left(\frac{p}{5}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 5, \\ -1, & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

For small odd primes, this gives the following comparison:

p	3	5	7	11	13	17	19	23	29	31	37
$\left(\frac{p}{5}\right)$	-1	–	-1	1	-1	-1	1	-1	1	1	-1
$\left(\frac{5}{p}\right)$	-1	–	-1	1	-1	-1	1	-1	1	1	-1.

These values suggest the conjecture

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

for odd primes $p \neq 5$.

Example 15.4 Compute $\left(\frac{7}{p}\right)$. We know that

$$\left(\frac{p}{7}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 2, 4 \pmod 7, \\ -1, & \text{if } p \equiv 3, 5, 6 \pmod 7. \end{cases}$$

For small odd primes, the comparison is

p	3	5	7	11	13	17	19	23	29	31	37
$\left(\frac{p}{7}\right)$	-1	-1	–	1	-1	-1	-1	1	1	-1	1
$\left(\frac{7}{p}\right)$	1	-1	–	-1	-1	-1	1	-1	1	1	1.

Theorem 15.5 (Law of quadratic reciprocity) Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Equivalently,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Example 15.6 By Theorem 15.5,

$$\left(\frac{5}{101}\right) = (-1)^{\frac{4}{2}\frac{100}{2}}\left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Combining this with the previous example gives $\left(\frac{90}{101}\right) = -1$.

Lemma 15.7 Let p be an odd prime, and let a be an odd integer with $\gcd(a,p) = 1$. Define

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Then

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}.$$

Proof. For each j with $1 \le j \le (p-1)/2$, choose the least nonnegative residue of ja modulo p. If the corresponding reduced residue in the interval $[-(p-1)/2, (p-1)/2]$ is negative, write that least nonnegative residue as $p + u_i$, where $u_i < 0$. If it is positive, write it as $v_w > 0$. Let there be

s negative residues and t positive residues. By Lemma 14.1,

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Using the division algorithm, we have

$$\begin{aligned}\sum_{j=1}^{(p-1)/2} ja &= p\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor + \sum_{i=1}^{s}(p+u_i) + \sum_{w=1}^{t} v_w \\ &= pT(a,p) + ps + \sum_{i=1}^{s} u_i + \sum_{w=1}^{t} v_w.\end{aligned}$$

The proof of Lemma 14.1 shows that

$$-u_1, -u_2, \ldots, -u_s, v_1, \ldots, v_t$$

are precisely the integers $1, 2, \ldots, (p-1)/2$. Hence

$$\sum_{j=1}^{(p-1)/2} j = -\sum_{i=1}^{s} u_i + \sum_{w=1}^{t} v_w.$$

Subtracting these two displayed equations gives

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) + ps + 2\sum_{i=1}^{s} u_i.$$

Since $a-1$ is even and p is odd, reducing modulo 2 gives

$$T(a,p) + s \equiv 0 \pmod 2.$$

Therefore $T(a,p) \equiv s \pmod 2$, so $(-1)^{T(a,p)} = (-1)^s = \left(\frac{a}{p}\right)$. □

Lecture 16 — Friday, October 23, 2015

Example 16.1 Using Lemma 15.7,

$$\begin{aligned} T(7,11) &= \sum_{j=1}^{5} \left\lfloor \frac{7j}{11} \right\rfloor \\ &= \left\lfloor \frac{7}{11} \right\rfloor + \left\lfloor \frac{14}{11} \right\rfloor + \left\lfloor \frac{21}{11} \right\rfloor + \left\lfloor \frac{28}{11} \right\rfloor + \left\lfloor \frac{35}{11} \right\rfloor \\ &= 0+1+1+2+3 \\ &= 7. \end{aligned}$$

Thus $\left(\frac{7}{11}\right) = (-1)^7 = -1$.

Example 16.2 There are two quick ways to compute $\left(\frac{11}{7}\right)$. First,

$$\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1.$$

Alternatively,

$$T(11,7) = \left\lfloor \frac{11}{7} \right\rfloor + \left\lfloor \frac{22}{7} \right\rfloor + \left\lfloor \frac{33}{7} \right\rfloor = 1+3+4 = 8,$$

so Lemma 15.7 gives $\left(\frac{11}{7}\right) = (-1)^8 = 1$.

Proof of Theorem 15.5. By Lemma 15.7,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(p,q)+T(q,p)}.$$

It is therefore enough to prove that

$$T(p,q) + T(q,p) = \frac{p-1}{2}\frac{q-1}{2}.$$

Consider the integer lattice points (x, y) satisfying

$$1 \le x \le \frac{p-1}{2} \qquad \text{and} \qquad 1 \le y \le \frac{q-1}{2}.$$

There are $\frac{p-1}{2}\frac{q-1}{2}$ such points. Since p and q are distinct primes, the equality $qx = py$ cannot occur in this rectangle: it would force $p \mid x$, but $0 < x < p$.

For a fixed y, the number of integers x in the rectangle with $qx < py$ is

$$\left\lfloor \frac{py}{q} \right\rfloor.$$

Thus the number of points with $qx < py$ is $T(p, q)$. Similarly, for a fixed x, the number of integers y in the rectangle with $py < qx$ is

$$\left\lfloor \frac{qx}{p} \right\rfloor,$$

so the number of points with $py < qx$ is $T(q, p)$. These two alternatives partition the rectangle, proving the displayed identity and hence the theorem. □

Example 16.3 We compute

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right).$$

For the first factor,

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) \\
&= \left(\frac{20}{23}\right) \\
&= \left(\frac{2^2 \cdot 5}{23}\right) \\
&= \left(\frac{5}{23}\right) \\
&= \left(\frac{23}{5}\right) \\
&= \left(\frac{3}{5}\right) \\
&= -1.
\end{aligned}$$

For the second factor,

$$\begin{aligned}\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right)\\ &= \left(\frac{17}{31}\right)\\ &= \left(\frac{31}{17}\right)\\ &= \left(\frac{14}{17}\right)\\ &= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right)\\ &= \left(\frac{7}{17}\right)\\ &= \left(\frac{17}{7}\right)\\ &= \left(\frac{3}{7}\right)\\ &= -1.\end{aligned}$$

Therefore

$$\left(\frac{713}{1009}\right) = (-1)(-1) = 1.$$

Lecture 17 — Monday, October 26, 2015

Definition 17.1 Let n be an odd positive integer with prime factorization

$$n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}.$$

If $\gcd(a, n) = 1$, the **Jacobi symbol** is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\cdots\left(\frac{a}{p_k}\right)^{t_k},$$

where the symbols on the right are Legendre symbols. For $n = 1$, we use the empty-product convention and set $(a/1) = 1$.

Theorem 17.2 Let n be an odd positive integer, and let a, b be integers coprime to n.

1. If $a \equiv b \pmod{n}$, then
$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$
2. We have
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$
3. If m is an odd positive integer with $\gcd(m, n) = 1$, then
$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

Proof. Write $n = p_1^{t_1} \cdots p_k^{t_k}$.

For (1), if $a \equiv b \pmod{n}$, then $a \equiv b \pmod{p_i}$ for each i. Hence $(a/p_i) = (b/p_i)$ for each i, and the result follows from Definition 17.1.

For (2), use the multiplicativity of the Legendre symbol in the numerator:

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{k}\left(\frac{ab}{p_i}\right)^{t_i} = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{t_i}\left(\frac{b}{p_i}\right)^{t_i} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

For (3), also write
$$m = q_1^{s_1} \cdots q_\ell^{s_\ell}.$$
The primes p_i and q_j are distinct because $\gcd(m, n) = 1$. Applying Theorem 15.5 to every pair gives

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right)^{s_j t_i}$$

$$= (-1)^{\left(\sum_{j=1}^{\ell} s_j \frac{q_j-1}{2}\right)\left(\sum_{i=1}^{k} t_i \frac{p_i-1}{2}\right)} \prod_{j=1}^{\ell}\prod_{i=1}^{k} \left(\frac{p_i}{q_j}\right)^{t_i s_j}$$
$$= (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right).$$

In the last step, we used the parity identities

$$\frac{m-1}{2} \equiv \sum_{j=1}^{\ell} s_j \frac{q_j-1}{2} \qquad \text{and} \qquad \frac{n-1}{2} \equiv \sum_{i=1}^{k} t_i \frac{p_i-1}{2} \pmod 2,$$

which follow by reducing the prime factorizations of m and n modulo 4. □

Warning The Jacobi symbol being equal to 1 does not imply that the corresponding quadratic congruence is solvable when the denominator is composite. For instance,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

but $x^2 \equiv 2 \pmod{15}$ has no solution because it has no solution modulo 3.

Example 17.3 Using the Jacobi symbol rules,

$$\begin{aligned}
\left(\frac{37503}{48611}\right) &= -\left(\frac{48611}{37503}\right) \\
&= -\left(\frac{11108}{37503}\right) \\
&= -\left(\frac{2777}{37503}\right) \\
&= -\left(\frac{1402}{2777}\right) \\
&= -\left(\frac{2}{2777}\right)\left(\frac{701}{2777}\right) \\
&= -\left(\frac{701}{2777}\right) \\
&= -\left(\frac{2777}{701}\right) \\
&= -\left(\frac{674}{701}\right)
\end{aligned}$$

$$
\begin{aligned}
&= -\left(\frac{2}{701}\right)\left(\frac{337}{701}\right) \\
&= \left(\frac{337}{701}\right) \\
&= \left(\frac{27}{337}\right) \\
&= \left(\frac{3}{337}\right)^3 \\
&= 1.
\end{aligned}
$$

The final equality follows from quadratic reciprocity, since $(3/337) = (337/3) = (1/3) = 1$.

Sums of Two Squares

Question 17.4 Which positive primes can be written as sums of two squares?

The small primes give the following table:

p	2	3	5	7	11	13	17	19	23	29
a^2+b^2	1^2+1^2	no	1^2+2^2	no	no	2^2+3^2	1^2+4^2	no	no	2^2+5^2

Theorem 17.5 (Fermat's theorem on sums of two squares) Let p be an odd prime. Then p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proof. *Forward implication.* Suppose that $p = a^2 + b^2$. Since p is odd, one of a, b is odd and the other is even. Without loss of generality, write $a = 2k+1$ and $b = 2\ell$. Then

$$p = (2k+1)^2 + (2\ell)^2 \equiv 1 \pmod 4.$$

We can also use quadratic reciprocity to give a more conceptual proof. If $p = a^2+b^2$, then $a^2 \equiv -b^2 \pmod p$, so

$$\left(\frac{a^2}{p}\right) = \left(\frac{-b^2}{p}\right) \implies \left(\frac{a}{p}\right)^2 = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right)^2 \implies 1 = \left(\frac{-1}{p}\right).$$

Neither a nor b is divisible by p: otherwise the congruence would force both to be divisible by

p, which is incompatible with $a^2 + b^2 = p$. Thus the Legendre symbols above are defined. By Theorem 13.2, the resulting equality implies $p \equiv 1 \pmod 4$.

Reverse implication. We use Fermat's method of infinite descent. Suppose that $p \equiv 1 \pmod 4$. By Theorem 13.2, the congruence

$$A^2 \equiv -1 \pmod p$$

has a solution. Choose A with $1 \leq A \leq (p-1)/2$. Then

$$A^2 + 1 = Mp$$

for some positive integer M. Since $p \geq 5$ and $A \leq (p-1)/2$, we have

$$M = \frac{A^2+1}{p} \leq \frac{(p-1)^2+4}{4p} < p.$$

If $M = 1$, we are done. If $M > 1$, Lemma 18.2 produces a representation $a^2 + b^2 = mp$ with $1 \leq m < M$. Repeating this descent eventually reaches $m = 1$, giving $p = a^2 + b^2$. □

Proposition 17.6 (Brahmagupta–Fibonacci identity) For all integers u, v, A, B,

$$(u^2+v^2)(A^2+B^2) = (uA+vB)^2 + (vA-uB)^2.$$

Proof. Expand the right-hand side:

$$(uA+vB)^2 + (vA-uB)^2 = u^2A^2 + v^2B^2 + v^2A^2 + u^2B^2 = (u^2+v^2)(A^2+B^2).$$

□

Lecture 18 — Wednesday, October 28, 2015

Example 18.1 Consider

$$387^2 + 1^2 = 170 \cdot 881.$$

We will descend from $M = 170$ to $M = 13$, and then from $M = 13$ to $M = 1$.

Solution. Choose $u = 47$ and $v = 1$, so that

$$u \equiv 387 \pmod{170} \qquad \text{and} \qquad v \equiv 1 \pmod{170},$$

with $-85 \leq u, v \leq 85$. Then

$$47^2 + 1^2 = 170 \cdot 13.$$

By Proposition 17.6,

$$(47^2 + 1^2)(387^2 + 1^2) = (47 \cdot 387 + 1)^2 + (1 \cdot 387 - 47)^2.$$

Both terms on the right are divisible by 170, so division by 170^2 gives

$$\left(\frac{47 \cdot 387 + 1}{170}\right)^2 + \left(\frac{387 - 47}{170}\right)^2 = 13 \cdot 881.$$

Thus

$$107^2 + 2^2 = 13 \cdot 881.$$

Now choose $u = 3$ and $v = 2$, so that $u \equiv 107 \pmod{13}$ and $v \equiv 2 \pmod{13}$. Since $3^2 + 2^2 = 13$, applying the identity again gives

$$\left(\frac{3 \cdot 107 + 2 \cdot 2}{13}\right)^2 + \left(\frac{2 \cdot 107 - 3 \cdot 2}{13}\right)^2 = 881.$$

Therefore

$$25^2 + 16^2 = 881.$$

□

Why does this algorithm always produce a smaller m with each iteration? The main point is that the integers u and v are chosen to be as small as possible in absolute value, so that $u^2 + v^2$ is not too large. The next lemma makes this precise.

Lemma 18.2 (Descent for sums of two squares) Let p be an odd prime, and suppose that

$$A^2 + B^2 = Mp$$

for integers A, B, M with $1 < M < p$. Then there exist integers a, b, m such that

$$a^2 + b^2 = mp \qquad \text{and} \qquad 1 \leq m < M.$$

Lecture 19 — Friday, October 30, 2015

Proof. Choose integers u and v satisfying

$$u \equiv A \pmod{M}, \qquad v \equiv B \pmod{M}, \qquad \text{and} \qquad -\frac{M}{2} \leq u, v \leq \frac{M}{2}.$$

Then

$$u^2 + v^2 \equiv A^2 + B^2 \equiv 0 \pmod{M},$$

so $u^2 + v^2 = mM$ for some nonnegative integer m. Also,

$$u^2 + v^2 \leq \frac{M^2}{4} + \frac{M^2}{4} = \frac{M^2}{2},$$

so $m \leq M/2 < M$. The case $m = 0$ would force $u = v = 0$, hence $M \mid A$ and $M \mid B$, which would force $M^2 \mid A^2 + B^2 = Mp$; since $1 < M < p$, this is impossible. Therefore $1 \leq m < M$.

Moreover,

$$uA + vB \equiv A^2 + B^2 \equiv 0 \pmod{M}$$

and

$$vA - uB \equiv BA - AB \equiv 0 \pmod{M}.$$

By Proposition 17.6,

$$(u^2 + v^2)(A^2 + B^2) = (uA + vB)^2 + (vA - uB)^2.$$

Substituting $u^2 + v^2 = mM$ and $A^2 + B^2 = Mp$, and then dividing by M^2, gives

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = mp.$$

This is the required smaller representation. □

Remark 19.1 The descent uses at most $O(\log M)$ iterations, since the value of M is at least halved at each step.

Question 19.2 This was all for primes. What kind of integers can be written as sums of two squares in general?

Example 19.3 The identity in Proposition 17.6 shows that a product of two sums of squares is again a sum of two squares. For example,

$$10 = (1^2 + 1^2)(1^2 + 2^2) = (1 \cdot 1 + 1 \cdot 2)^2 + (1 \cdot 1 - 1 \cdot 2)^2 = 3^2 + 1^2.$$

Similarly,

$$130 = 2 \cdot 5 \cdot 13 = (1^2 + 1^2)(2^2 + 1^2)(2^2 + 3^2) = 9^2 + 7^2.$$

Also, $121 = 11^2 + 0^2$, even though $11 \equiv 3 \pmod 4$ is not itself a sum of two squares.

Theorem 19.4 A positive integer n is a sum of two squares if and only if

$$n = p_1 \cdots p_l M^2,$$

where $M \in \mathbb{N}$ and $p_1, \ldots, p_l$ are distinct primes with $p_i \not\equiv 3 \pmod 4$.

Proof. *Reverse implication.* The prime 2 is a sum of two squares, every prime $p_i \equiv 1 \pmod 4$ is a sum of two squares by Theorem 17.5, and products of sums of two squares are sums of two squares by Proposition 17.6.

Forward implication. Suppose $n = a^2 + b^2$. Let $d = \gcd(a, b)$, and write $a = da_0$ and $b = db_0$ with $\gcd(a_0, b_0) = 1$. Then

$$n = d^2(a_0^2 + b_0^2).$$

It suffices to prove the following claim.

Claim. If $m = a^2 + b^2$ with $\gcd(a, b) = 1$, then either m is odd and all prime factors of m are congruent to 1 modulo 4, or m is even and $m/2$ is a product of odd primes congruent to 1 modulo 4.

To prove the claim, let p be an odd prime factor of m. Then $m = a^2 + b^2$ gives

$$a^2 + b^2 \equiv 0 \pmod p,$$

so

$$a^2 \equiv -b^2 \pmod p.$$

Since $\gcd(a,b)=1$, the prime p divides neither a nor b. Therefore

$$\left(\frac{a}{p}\right)^2 = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right)^2,$$

and hence $1 = \left(\frac{-1}{p}\right)$. By Theorem 13.2, this forces $p \equiv 1 \pmod 4$.

If m is odd, the claim follows. If m is even, then a and b must both be odd because $\gcd(a,b)=1$. Thus $a = 2k+1$ and $b = 2l+1$ for some $k, l \in \mathbb{Z}$, and

$$\begin{aligned} m = a^2 + b^2 &= (2k+1)^2 + (2l+1)^2 \\ &= 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \\ &= 4(k^2 + k + l^2 + l) + 2. \end{aligned}$$

Therefore

$$\frac{m}{2} = 2(k^2 + k + l^2 + l) + 1$$

is odd. Since all odd prime factors of m are congruent to 1 modulo 4, the claim is proved.

Applying the claim to $a_0^2 + b_0^2$ shows that every prime factor of this number is either 2 or congruent to 1 modulo 4, and that the exponent of 2 is at most one. In its prime factorization, extract one copy of each prime having odd exponent and absorb every remaining even power, together with d^2, into a square M^2. The extracted primes are distinct and none is congruent to 3 modulo 4, so n has the required form. □

Remark 19.5 In the proof, the Legendre symbols $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are defined because $\gcd(a,b)=1$ and $p \mid a^2+b^2$ imply that p divides neither a nor b.

Lecture 20 — Monday, November 02, 2015

Summary of Congruence Tools

This review has two recurring goals: identify the relevant arithmetic obstruction, and keep the computational steps distinct.

1. **Pythagorean triples.** To find the integer solutions of

$$a^2 + b^2 = c^2,$$

first reduce to primitive Pythagorean triples. A triple (a, b, c) is primitive if $\gcd(a, b, c) = 1$. Up to swapping a and b and changing signs, Theorem 2.2 says that the positive primitive triples are exactly

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad c = \frac{s^2 + t^2}{2},$$

where $s > t$ are odd coprime positive integers. The general positive triples are obtained by multiplying all three entries by a common positive integer M.

2. **Fermat and Euler.** If p is prime and $(a, p) = 1$, then Fermat's little theorem gives

$$a^{p-1} \equiv 1 \pmod{p}.$$

More generally, if $(a, m) = 1$, then Euler's theorem gives

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

If

$$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r},$$

then

$$\phi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Thus computing $\phi(m)$ requires the prime factorization of m.

3. **Successive squaring.** To compute a large power modulo m, write the exponent in binary and square successively. For example, to compute $9^{53} \pmod{67}$, write

$$53 = 2^5 + 2^4 + 2^2 + 2^0.$$

Then

$$\begin{aligned}
9^2 &\equiv 81 \equiv 14 \pmod{67}, \\
9^4 &\equiv 14^2 \equiv 62 \pmod{67}, \\
9^8 &\equiv 62^2 \equiv 25 \pmod{67}, \\
9^{16} &\equiv 25^2 \equiv 22 \pmod{67}, \\
9^{32} &\equiv 22^2 \equiv 15 \pmod{67}.
\end{aligned}$$

Therefore

$$9^{53} = 9^{32+16+4+1} \equiv 15 \cdot 22 \cdot 62 \cdot 9 \equiv 24 \pmod{67}.$$

4. Taking kth roots modulo m. To solve

$$x^k \equiv b \pmod{m},$$

suppose that $(b, m) = 1$ and $\gcd(k, \phi(m)) = 1$. Choose $u, v \in \mathbb{Z}$ such that

$$ku - v\phi(m) = 1.$$

Then $x \equiv b^u \pmod{m}$ is a solution, because

$$(b^u)^k = b^{ku} = b^{1+v\phi(m)} = b\left(b^{\phi(m)}\right)^v \equiv b \pmod{m}.$$

This method is not a general solution method when $\gcd(k, \phi(m)) \neq 1$.

5. Primitive roots and indices. For $(a, p) = 1$, the smallest positive integer n such that

$$a^n \equiv 1 \pmod{p}$$

is the exponent $e_p(a)$. The primitive root theorem says that, for every prime p, there is a g with $e_p(g) = p - 1$. Such a g is a primitive root modulo p, and

$$\{g, g^2, \ldots, g^{p-1}\} \pmod{p}$$

is the set of nonzero residue classes modulo p in some order. Once a primitive root g is fixed, the index $I(a)$ is defined by

$$a \equiv g^{I(a)} \pmod{p}.$$

The index rules are

$$I(ab) \equiv I(a) + I(b) \pmod{p-1} \qquad \text{and} \qquad I(a^k) \equiv kI(a) \pmod{p-1}.$$

6. Index method for kth roots modulo primes. To solve

$$x^k \equiv b \pmod{p}$$

with $(b, p) = 1$ and $\gcd(k, p - 1) = 1$, use indices:

$$I(x^k) \equiv I(b) \pmod{p-1}.$$

Hence

$$kI(x) \equiv I(b) \pmod{p-1},$$

so

$$I(x) \equiv k^{-1} I(b) \pmod{p-1},$$

where k^{-1} is the inverse of k modulo $p-1$.

7. **Legendre symbols.** The method above breaks for square roots modulo an odd prime p, since $\gcd(2, p-1) \neq 1$. For nonzero a modulo p, the Legendre symbol is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution,} \\ -1, & \text{otherwise.} \end{cases}$$

8. **Quadratic reciprocity.** For odd primes, the main computational rules are

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

and, for distinct odd primes p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The Legendre symbol is also multiplicative:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Lecture 21 — Wednesday, November 04, 2015

4. Pell Equations and Gaussian Integers

Pell Equations and Infinite Descent

Definition 21.1 The **triangular numbers** are those of the form

$$T_m = 1 + 2 + \cdots + m = \frac{m(m+1)}{2}.$$

Question 21.2 Which triangular numbers are squares? That is, what are the positive integer solutions of

$$n^2 = \frac{m(m+1)}{2}?$$

The first few values are

n^2	1	4	9	16	25	36	49	64	81	100
T_m	1	3	6	10	15	21	28	36	45	55.

The first square triangular numbers are 1, 36, and $1225 = 35^2$. They grow very fast, and there is no obvious pattern.

We can at least put the equation into a more useful form. Multiplying

$$n^2 = \frac{m(m+1)}{2}$$

by 8 gives

$$8n^2 = 4m(m+1) = 4m^2 + 4m = (2m+1)^2 - 1.$$

Thus

$$2(2n)^2 = (2m+1)^2 - 1.$$

If

$$y = 2n \qquad \text{and} \qquad x = 2m+1,$$

then the square triangular problem becomes

$$x^2 - 2y^2 = 1.$$

Conversely, a positive solution of this equation with x odd and y even recovers

$$n = \frac{y}{2} \qquad \text{and} \qquad m = \frac{x-1}{2}.$$

For example,

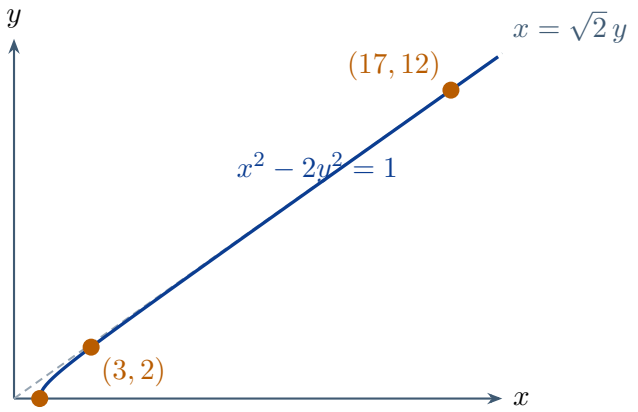
$$(n, m) = (1, 1),\ (6, 8),\ (35, 49)$$

correspond to

$$(x, y) = (3, 2),\ (17, 12),\ (99, 70).$$

The first two nontrivial lattice points on the positive branch of $x^2 - 2y^2 = 1$ appear in Figure 8. The curve approaches the asymptote $x = \sqrt{2}\, y$, so its integer points encode exceptionally accurate

rational approximations x/y to $\sqrt{2}$.



Pell solutions are the sparse integer points lying exactly on the hyperbola

FIGURE 8

The factorization

$$x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$$

suggests looking at the numbers $x + y\sqrt{2}$. Since

$$1 = (3 - 2\sqrt{2})(3 + 2\sqrt{2}),$$

squaring preserves the equation:

$$1 = (3 - 2\sqrt{2})^2(3 + 2\sqrt{2})^2 = (17 - 12\sqrt{2})(17 + 12\sqrt{2}) = 17^2 - 2 \cdot 12^2.$$

Cubing similarly gives

$$(3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2},$$

and hence another solution $(x, y) = (99, 70)$. This motivates the following theorem.

Theorem 21.3 Let x_k and y_k be the positive integers defined by

$$(3 + 2\sqrt{2})^k = x_k + y_k\sqrt{2} \quad (k \geq 1).$$

Then the following hold.

1. The positive integer solutions of

$$x^2 - 2y^2 = 1$$

are precisely (x_k, y_k) for $k \geq 1$.

2. The positive square triangular numbers are precisely

$$n_k^2 = \left(\frac{y_k}{2}\right)^2 \qquad \text{and} \qquad m_k = \frac{x_k - 1}{2},$$

where $k \geq 1$.

Proof. The preliminary discussion shows that the square triangular problem is equivalent to the Pell equation

$$x^2 - 2y^2 = 1$$

with $x = 2m + 1$ and $y = 2n$. Conversely, if $x^2 - 2y^2 = 1$ with $x, y > 0$, then x is odd. Hence $x^2 \equiv 1 \pmod 8$, so $2y^2 = x^2 - 1$ is divisible by 8, and therefore y is even. Thus

$$m = \frac{x-1}{2} \qquad \text{and} \qquad n = \frac{y}{2}$$

are integers and give a square triangular number. This proves (2) once (1) is known.

It remains to prove (1). Since

$$(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1,$$

every power $(3 + 2\sqrt{2})^k = x_k + y_k\sqrt{2}$ satisfies

$$x_k^2 - 2y_k^2 = 1.$$

For example,

$$(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} \qquad \text{and} \qquad (3 + 2\sqrt{2})^3 = 99 + 70\sqrt{2}.$$

We now prove that no other positive solutions occur. Let (u, v) be a positive solution of $u^2 - 2v^2 = 1$. The smallest positive solution is $(3, 2)$: the case $v = 1$ gives no integer u, and $v = 2$ gives $u = 3$.

The descent claim is the following. If $(u, v) \neq (3, 2)$, so that $u > 3$, then there are positive integers s, t such that

$$s < u, \qquad s^2 - 2t^2 = 1, \qquad \text{and} \qquad u + v\sqrt{2} = (3 + 2\sqrt{2})(s + t\sqrt{2}).$$

To verify the claim, solve for s and t from the last equation. Expanding gives

$$u = 3s + 4t \qquad \text{and} \qquad v = 2s + 3t,$$

and hence

$$s = 3u - 4v \qquad \text{and} \qquad t = 3v - 2u.$$

Taking norms in

$$u + v\sqrt{2} = (3 + 2\sqrt{2})(s + t\sqrt{2})$$

then gives

$$s^2 - 2t^2 = 1.$$

It remains to check that $s > 0$, $t > 0$, and $s < u$. For $s > 0$, the equation $u^2 = 2v^2 + 1$ gives

$$\frac{u}{v} > \sqrt{2} > \frac{4}{3},$$

so

$$s = 3u - 4v = 3v\left(\frac{u}{v} - \frac{4}{3}\right) > 0.$$

For $t > 0$, note that $2v^2 = u^2 - 1$. Multiplying by $9/2$ gives

$$9v^2 = \frac{9}{2}u^2 - \frac{9}{2} = 4u^2 + \frac{1}{2}(u^2 - 9).$$

Since $u > 3$, this implies

$$9v^2 > 4u^2,$$

so $3v > 2u$ and $t = 3v - 2u > 0$. Finally, since $u = 3s + 4t$ and $s, t > 0$, we have $s < u$. This proves the claim.

This descent can be repeated until the first coordinate is 3. Therefore

$$u + v\sqrt{2} = (3 + 2\sqrt{2})^k$$

for some $k \geq 1$, as required. □

Lecture 22 — Friday, November 06, 2015

Pell Equations

Definition 22.1 Let D be a positive integer that is not a perfect square. The equation

$$x^2 - Dy^2 = 1$$

is called a **Pell equation**.

The condition that D is not a square is essential. If $D = d^2$, then

$$x^2 - d^2y^2 = (x + dy)(x - dy) = 1,$$

so the equation has only the elementary factorizations coming from the two integer factors of 1. When D is not a square, the equation is symmetric under changing signs of x and y, so we concentrate on positive solutions.

Proposition 22.2 If (x_0, y_0) is a positive solution of $x^2 - Dy^2 = 1$, then

$$x_1 = x_0^2 + Dy_0^2 \qquad \text{and} \qquad y_1 = 2x_0y_0$$

also gives a positive solution. Consequently, one nontrivial solution produces infinitely many solutions.

Proof. Since

$$(x_0 + y_0\sqrt{D})(x_0 - y_0\sqrt{D}) = 1,$$

squaring gives

$$(x_0 + y_0\sqrt{D})^2 = (x_0^2 + Dy_0^2) + 2x_0y_0\sqrt{D}.$$

Similarly,

$$(x_0 - y_0\sqrt{D})^2 = (x_0^2 + Dy_0^2) - 2x_0y_0\sqrt{D}.$$

Thus, with $x_1 = x_0^2 + Dy_0^2$ and $y_1 = 2x_0y_0$,

$$1 = (x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D}) = x_1^2 - Dy_1^2.$$

Moreover, $x_1 = 2x_0^2 - 1 > x_0$ because a positive solution has $x_0 > 1$. Iterating the construction therefore gives solutions with strictly increasing first coordinates, so the solutions are distinct. $\square$

Remark 22.3 The smallest positive solution can be surprisingly large. For example, the smallest positive solution of

$$x^2 - 313y^2 = 1$$

has

$$(x, y) = (32188120829134849, 1819380158564160).$$

The smallest positive solution of

$$x^2 - 61y^2 = 1$$

is

$$(x, y) = (1766319049, 226153980).$$

For $D = 47$ the smallest positive solution is $(48, 7)$, and for $D = 73$ it is $(2281249, 267000)$.

Our main structural theorem says that every positive solution is generated from the smallest one. There are two steps: first prove that a positive solution exists, and then prove that all positive solutions are powers of the smallest one.

Factoring the Pell equation gives

$$(x - y\sqrt{D})(x + y\sqrt{D}) = 1.$$

For positive x, y, the factor $x - y\sqrt{D}$ must therefore be very small. Equivalently, we want rational approximations x/y to $\sqrt{D}$ satisfying a bound of the form

$$\left| \frac{x}{y} - \sqrt{D} \right| < \frac{1}{y^2}.$$

For any fixed positive y, choosing x to be the closest integer to $y\sqrt{D}$ only gives

$$\left| x - y\sqrt{D} \right| < \frac{1}{2}.$$

The next theorem gives a much stronger approximation for infinitely many values of y.

Theorem 22.4 (Pigeonhole principle) If more than n objects are placed into n boxes, then at least one box contains more than one object.

Theorem 22.5 (Dirichlet Diophantine approximation theorem) Let α be irrational. Then there are infinitely many pairs (x, y) with $x \in \mathbb{Z}$ and $y \in \mathbb{N}$ such that

$$|x - y\alpha| < \frac{1}{y}.$$

Equivalently,

$$\left|\frac{x}{y} - \alpha\right| < \frac{1}{y^2}.$$

Proof. Fix a positive integer Y. Partition $[0, 1)$ into the Y half-open intervals

$$\left[0, \frac{1}{Y}\right), \left[\frac{1}{Y}, \frac{2}{Y}\right), \ldots, \left[\frac{Y-1}{Y}, 1\right).$$

For $j = 0, 1, \ldots, Y$, write

$$j\alpha = N_j + F_j, \qquad N_j = \lfloor j\alpha \rfloor, \qquad \text{and} \qquad 0 \le F_j < 1.$$

There are $Y + 1$ numbers F_j and only Y intervals, so two of them lie in the same interval. Say $0 \le n < m \le Y$. Then

$$|F_m - F_n| < \frac{1}{Y}.$$

With $y = m - n$ and $x = N_m - N_n$, this gives

$$|x - y\alpha| < \frac{1}{Y} \qquad \text{and} \qquad 1 \le y \le Y.$$

This produces infinitely many values of y. If only finitely many occurred, only finitely many corresponding x could occur under the bound $|x - y\alpha| < 1/y$, so the nonzero errors $|x - y\alpha|$ among them would have a positive minimum because α is irrational. Choosing Y larger than the reciprocal of that minimum gives a contradiction. Since $y \le Y$, the inequality above implies

$$|x - y\alpha| < \frac{1}{Y} \le \frac{1}{y}.$$

□

Lecture 23 — Monday, November 09, 2015

Example 23.1 We can find positive integers x, y such that

$$\left|x - y\sqrt{13}\right| < \frac{1}{5}.$$

Write $j\sqrt{13} = N_j + F_j$ for $j = 0, 1, \ldots, 5$, where $N_j = \lfloor j\sqrt{13} \rfloor$ and $0 \leq F_j < 1$. The values $F_0, \ldots, F_5$ are six numbers in $[0, 1)$, and the five half-open intervals

$$\left[0, \frac{1}{5}\right), \left[\frac{1}{5}, \frac{2}{5}\right), \left[\frac{2}{5}, \frac{3}{5}\right), \left[\frac{3}{5}, \frac{4}{5}\right), \left[\frac{4}{5}, 1\right)$$

force two of them to lie in the same interval. In this case $F_0 = 0$ and

$$F_5 = 5\sqrt{13} - 18 \approx 0.0278$$

are already close, so

$$\left|18 - 5\sqrt{13}\right| < \frac{1}{5}.$$

Lemma 23.2 Let D be a positive nonsquare integer. There are infinitely many positive integer pairs (x, y) such that

$$0 < \left|x^2 - Dy^2\right| < 2\sqrt{D} + 1.$$

Consequently, there is a nonzero integer M for which

$$x^2 - Dy^2 = M$$

has infinitely many positive integer solutions.

Proof. Apply Theorem 22.5 with $\alpha = \sqrt{D}$. It initially gives $x \in \mathbb{Z}$ and $y > 0$, with infinitely many distinct values of y. For all sufficiently large such y,

$$\frac{x}{y} > \sqrt{D} - \frac{1}{y^2} > 0,$$

so discarding finitely many pairs leaves infinitely many positive integer pairs (x, y) such that

$$\left|x - y\sqrt{D}\right| < \frac{1}{y}.$$

For these pairs,

$$\left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{y^2},$$

so $x/y < \sqrt{D} + 1/y^2$. Hence

$$\begin{aligned}
\left|x^2 - Dy^2\right| &= \left|x - y\sqrt{D}\right|\left|x + y\sqrt{D}\right| \\
&< \frac{1}{y}\left(x + y\sqrt{D}\right) \\
&= \frac{x}{y} + \sqrt{D} \\
&< 2\sqrt{D} + \frac{1}{y^2} \\
&\leq 2\sqrt{D} + 1.
\end{aligned}$$

The value $x^2 - Dy^2$ is never zero, because D is not a square. Since there are only finitely many nonzero integers with absolute value less than $2\sqrt{D} + 1$, one of them occurs infinitely often. □

Lecture 24 — Wednesday, November 11, 2015

Example 24.1 For $D = 13$, the equation

$$x^2 - 13y^2 = 4$$

has solutions such as

$$(11, 3), \qquad (119, 33), \qquad \text{and} \qquad (14159, 3927).$$

Dividing two corresponding numbers in $\mathbb{Z}[\sqrt{13}]$ can produce a solution of the Pell equation,

but the quotient need not have integer coefficients. For instance,

$$\begin{aligned}\frac{119-33\sqrt{13}}{11-3\sqrt{13}} &= \frac{(119-33\sqrt{13})(11+3\sqrt{13})}{(11-3\sqrt{13})(11+3\sqrt{13})}\\ &= \frac{22-6\sqrt{13}}{4},\end{aligned}$$

so this quotient does not work. Trying the next solution gives

$$\begin{aligned}\frac{14159-3927\sqrt{13}}{11-3\sqrt{13}} &= \frac{(14159-3927\sqrt{13})(11+3\sqrt{13})}{(11-3\sqrt{13})(11+3\sqrt{13})}\\ &= 649-180\sqrt{13}.\end{aligned}$$

Thus

$$649^2 - 13\cdot 180^2 = 1.$$

Theorem 24.2 (Pell equation theorem: part 1) Let D be a positive integer that is not a perfect square. Then the Pell equation

$$x^2 - Dy^2 = 1$$

has a solution in positive integers.

Proof. By Lemma 23.2, there is a nonzero integer M for which

$$x^2 - Dy^2 = M$$

has infinitely many positive integer solutions. Set up the pigeonholes using the residue classes

$$(A,B), \quad 0 \le A, B < |M|,$$

and place a solution (x,y) into the pigeonhole determined by

$$x \equiv A \pmod{|M|}, \qquad \text{and} \qquad y \equiv B \pmod{|M|}.$$

Since there are infinitely many solutions and only finitely many pigeonholes, there are two distinct positive solutions (x_i, y_i) and (x_j, y_j) in the same pigeonhole. Thus

$$x_i \equiv x_j \pmod{|M|} \qquad \text{and} \qquad y_i \equiv y_j \pmod{|M|}.$$

As the solutions are distinct and positive, both coordinates differ: equality of either positive coordinate in $x^2 - Dy^2 = M$ would force equality of the other.

Now form the quotient

$$\begin{aligned} X + Y\sqrt{D} &= \frac{x_i - y_i\sqrt{D}}{x_j - y_j\sqrt{D}} \\ &= \frac{(x_i - y_i\sqrt{D})(x_j + y_j\sqrt{D})}{x_j^2 - Dy_j^2} \\ &= \frac{x_i x_j - D y_i y_j}{M} + \frac{x_i y_j - x_j y_i}{M}\sqrt{D}. \end{aligned}$$

Thus

$$X = \frac{x_i x_j - D y_i y_j}{M} \qquad \text{and} \qquad Y = \frac{x_i y_j - x_j y_i}{M}.$$

Taking norms gives

$$X^2 - DY^2 = \frac{x_i^2 - Dy_i^2}{x_j^2 - Dy_j^2} = \frac{M}{M} = 1.$$

However, we still need to check that $X, Y \in \mathbb{Z}$ and $Y \neq 0$. For integrality, the congruences above give

$$x_i x_j - D y_i y_j \equiv x_i^2 - D y_i^2 \equiv M \equiv 0 \pmod{|M|},$$

so $X \in \mathbb{Z}$. Similarly,

$$x_i y_j - x_j y_i \equiv x_i y_i - x_i y_i \equiv 0 \pmod{|M|},$$

so $Y \in \mathbb{Z}$.

Finally, suppose for a contradiction that $Y = 0$. Then $x_i y_j = x_j y_i$, and hence

$$\begin{aligned} y_j^2 M &= y_j^2(x_i^2 - D y_i^2) \\ &= (x_i y_j)^2 - D(y_i y_j)^2 \\ &= (x_j y_i)^2 - D(y_i y_j)^2 \\ &= y_i^2(x_j^2 - D y_j^2) \\ &= y_i^2 M. \end{aligned}$$

Since $M \neq 0$ and $y_i, y_j > 0$, this forces $y_i = y_j$, contradicting the choice of distinct solutions. Thus $Y \neq 0$.

The equation $X^2 - DY^2 = 1$ also forces $X \neq 0$. Therefore $(|X|, |Y|)$ is a positive solution of the Pell equation. □

Theorem 24.3 (Pell equation theorem: part 2) Let (x_1, y_1) be the positive solution of $x^2 - Dy^2 = 1$ with the smallest positive first coordinate. Then every positive solution (u, v) has the form

$$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})^k$$

for some integer $k \geq 1$. Conversely, every such power gives a positive solution.

Lecture 25 — Friday, November 13, 2015

Proof. For the converse, expanding any positive power of $x_1 + y_1\sqrt{D}$ gives positive integer coefficients, and multiplicativity of the norm shows that those coefficients solve the Pell equation. We prove that every positive solution is obtained this way by descent.

The claim is the following. If (u, v) is a positive solution of $x^2 - Dy^2 = 1$ with $u > x_1$, then there are positive integers s, t such that

$$s < u \qquad \text{and} \qquad u + v\sqrt{D} = (x_1 + y_1\sqrt{D})(s + t\sqrt{D}).$$

Assuming the claim, the proof is immediate. Starting with any positive solution (u, v), if $u = x_1$, then $v = y_1$, because $Dv^2 = u^2 - 1 = Dy_1^2$ and both v and y_1 are positive. If $u > x_1$, the claim gives a smaller positive solution (s, t). Repeating the descent eventually reaches (x_1, y_1), and multiplying the factors back gives

$$u + v\sqrt{D} = (x_1 + y_1\sqrt{D})^k$$

for some $k \geq 1$.

It remains to prove the claim. Expanding the desired factorization gives

$$u = x_1 s + Dy_1 t \qquad \text{and} \qquad v = x_1 t + y_1 s.$$

Solving this linear system, whose determinant is $x_1^2 - Dy_1^2 = 1$, gives

$$s = x_1 u - Dy_1 v \qquad \text{and} \qquad t = x_1 v - y_1 u.$$

Taking norms in the factorization gives $s^2 - Dt^2 = 1$ once s and t are defined this way.

We now check that $s > 0$, $t > 0$, and $s < u$. Since

$$\frac{u}{v} > \sqrt{D}$$

we have

$$s = x_1 u - D y_1 v > x_1 v\sqrt{D} - D y_1 v = v\sqrt{D}(x_1 - y_1\sqrt{D}).$$

Also

$$(x_1 - y_1\sqrt{D})(x_1 + y_1\sqrt{D}) = 1,$$

so $x_1 - y_1\sqrt{D} > 0$. Hence $s > 0$.

For $t > 0$, we need to show $x_1 v > y_1 u$. Since all quantities are positive, this is equivalent to

$$x_1^2 v^2 > y_1^2 u^2.$$

Using $Dv^2 = u^2 - 1$ and $Dy_1^2 = x_1^2 - 1$, this inequality becomes

$$x_1^2(u^2 - 1) > (x_1^2 - 1)u^2,$$

which is equivalent to $u^2 > x_1^2$. This holds because $u > x_1$.

Finally,

$$u = x_1 s + D y_1 t > s,$$

since s, t, x_1, y_1, D are positive. This proves the claim, and hence the theorem. □

The preceding theorem completes the Pell equation analysis that began with square triangular numbers. We now turn to a different quadratic extension of the integers, namely the Gaussian integers.

Gaussian Integers

The polynomial

$$x^2 - 3x + 2 = (x - 1)(x - 2)$$

has real roots, but

$$x^2 + 1$$

has no real root. To keep solving polynomial equations, we enlarge the real numbers by adjoining a square root of -1.

Definition 25.1 Let i be a symbol satisfying $i^2 = -1$. The **complex numbers** are

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

with addition and multiplication defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Theorem 25.2 (Fundamental theorem of algebra) Every nonconstant polynomial with complex coefficients has a root in $\mathbb{C}$.

Definition 25.3 The **Gaussian integers** are

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

The set $\mathbb{Z}[i]$ is closed under addition and multiplication. Division need not stay inside $\mathbb{Z}[i]$:

$$\frac{3 + 4i}{1 - 2i} = \frac{(3 + 4i)(1 + 2i)}{(1 - 2i)(1 + 2i)} = -1 + 2i \in \mathbb{Z}[i],$$

but

$$\frac{6 + 13i}{1 - 2i} = -\frac{14}{5} + \frac{23}{5}i \notin \mathbb{Z}[i].$$

We therefore need a division algorithm with a remainder, just as in $\mathbb{Z}$. In $\mathbb{Z}$, the division algorithm lets us measure the "failure" of division by the size of the remainder. What about in $\mathbb{Z}[i]$?

Lecture 26 — Monday, November 16, 2015

Question 26.1 Can elements of $\mathbb{Z}[i]$ be factored in a useful way?

Definition 26.2 Let $\alpha \in \mathbb{Z}[i]$.

1. The element α is a **unit** if there is some $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$.
2. A nonzero nonunit α is **irreducible** if every factorization $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$ has either β or γ a unit.
3. A nonzero nonunit α is **prime** if $\alpha \mid \beta\gamma$ implies $\alpha \mid \beta$ or $\alpha \mid \gamma$.

Definition 26.3 For $\alpha = a + bi \in \mathbb{Z}[i]$, the **norm** of α is

$$N(\alpha) = \alpha\overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

Proposition 26.4 For all $\alpha, \beta \in \mathbb{Z}[i]$,

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof. This follows from complex conjugation:

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\,\overline{\beta} = \alpha\overline{\alpha}\,\beta\overline{\beta} = N(\alpha)N(\beta).$$

□

Proposition 26.5 The units in $\mathbb{Z}[i]$ are

$$1,\ -1,\ i,\ -i.$$

Equivalently, α is a unit if and only if $N(\alpha) = 1$.

Proof. Let $\alpha = a + bi$ be a unit. Then $\alpha^{-1} \in \mathbb{Z}[i]$, but

$$\alpha^{-1} = \frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

Thus

$$\frac{a}{a^2 + b^2} \in \mathbb{Z} \qquad \text{and} \qquad \frac{b}{a^2 + b^2} \in \mathbb{Z}.$$

Also

$$|a| \leq a^2 + b^2 \qquad \text{and} \qquad |b| \leq a^2 + b^2.$$

Therefore each of the two displayed fractions is either 0, 1, or -1. If $a = 0$, then $b = \pm 1$, so $\alpha = \pm i$. If $b = 0$, then $a = \pm 1$, so $\alpha = \pm 1$. If both a and b are nonzero, then $a^2 + b^2 > |a|$ and $a^2 + b^2 > |b|$, so neither fraction can be a nonzero integer. Hence this case is impossible.

Thus the only units are $1, -1, i, -i$, and each of these is visibly a unit. The equivalence with $N(\alpha) = 1$ follows because these four elements have norm 1, and $a^2 + b^2 = 1$ with $a, b \in \mathbb{Z}$ forces $(a, b) = (\pm 1, 0)$ or $(0, \pm 1)$. □

Example 26.6 In $\mathbb{Z}[i]$, the integer 6 factors as

$$6 = 2 \cdot 3 = (1 + i)(1 - i) \cdot 3 = -i(1 + i)^2 \cdot 3.$$

The factor 2 is reducible, while the factor 3 remains irreducible.

We can check this directly. Suppose first that

$$2 = (a + bi)(c + di) = (ac - bd) + (bc + ad)i.$$

Then

$$2 = ac - bd \qquad \text{and} \qquad 0 = bc + ad.$$

Multiplying the first equation by b and using $bc = -ad$ gives

$$2b = abc - b^2 d = -a^2 d - b^2 d = -(a^2 + b^2)d.$$

If $a = 0$ or $b = 0$, then one of the two factors is a unit. Otherwise assume $a, b \neq 0$, and after interchanging the two factors if necessary assume $|b| \leq |d|$. Then

$$2|b| = (a^2 + b^2)|d| \geq (a^2 + b^2)|b|,$$

so $a^2 + b^2 \leq 2$. Since a and b are both nonzero, this forces

$$a^2 + b^2 = 2,$$

and hence $a = \pm 1$ and $b = \pm 1$. Thus the only nontrivial factorization of 2 is, up to multiplication by units,

$$2 = (1 + i)(1 - i) = -i(1 + i)^2.$$

Now suppose

$$3 = (a + bi)(c + di).$$

The same calculation gives

$$3b = -(a^2 + b^2)d.$$

Again, if $a = 0$ or $b = 0$, then one factor is a unit. If $a, b \neq 0$ and $|b| \leq |d|$, then $a^2 + b^2 \leq 3$. The value $a^2 + b^2 = 2$ would make $3|b| = 2|d|$, impossible. The value $a^2 + b^2 = 3$ has no integer solutions with $a, b \neq 0$. Hence every factorization of 3 has a unit factor, so 3 is irreducible in $\mathbb{Z}[i]$.

Theorem 26.7 Let p be a prime in $\mathbb{Z}$. As an element of $\mathbb{Z}[i]$, p is irreducible if and only if

$$p \equiv 3 \pmod 4.$$

Proof. If $p = 2$, then $2 = (1 + i)(1 - i)$, and neither factor is a unit. Hence 2 is reducible.

If $p \equiv 1 \pmod 4$, then Theorem 17.5 gives $p = a^2 + b^2$ with $a, b > 0$, so

$$p = (a + bi)(a - bi)$$

is a nontrivial factorization in $\mathbb{Z}[i]$.

It remains to prove that primes $p \equiv 3 \pmod 4$ are irreducible. Suppose

$$p = (a + bi)(c + di).$$

If neither factor is a unit, then both factors have norm greater than 1. Taking norms gives

$$p^2 = (a^2 + b^2)(c^2 + d^2),$$

so primality forces

$$a^2 + b^2 = p.$$

But a square is congruent to 0 or 1 modulo 4, and a sum of two squares cannot be congruent to 3 modulo 4. This contradiction shows that one of the factors must be a unit. Thus p is irreducible. □

Lecture 27 — Wednesday, November 18, 2015

Proposition 27.1 Every prime element of $\mathbb{Z}[i]$ is irreducible.

Proof. Let α be prime and suppose $\alpha = \beta\gamma$. Since $\alpha \mid \beta\gamma$, primality gives $\alpha \mid \beta$ or $\alpha \mid \gamma$. If $\alpha \mid \beta$, then $\beta = \alpha\delta$ for some $\delta \in \mathbb{Z}[i]$, and hence

$$\alpha = \alpha\delta\gamma.$$

Cancelling the nonzero element α gives $\delta\gamma = 1$, so γ is a unit. The case $\alpha \mid \gamma$ is symmetric. □

Remark 27.2 The converse is false in general rings. For contrast, consider

$$\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}.$$

If $x + y\sqrt{3}$ is a unit, then its norm $x^2 - 3y^2$ must be 1 or -1. The value -1 is impossible modulo 3, so

$$x^2 - 3y^2 = 1.$$

Thus even describing the units leads back to a Pell equation.

Unique factorization can also fail. For instance, in

$$\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\},$$

one visible failure is

$$4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1).$$

The factors 2, $\sqrt{5} - 1$, and $\sqrt{5} + 1$ can be checked to be irreducible but not prime. Indeed, their norms are $4, -4, -4$. A nontrivial factorization of any one of them would require a factor of norm 2 or -2, but $x^2 - 5y^2 \equiv \pm 2 \pmod 5$ has no solution. On the other hand, 2 divides $(\sqrt{5} - 1)(\sqrt{5} + 1) = 4$ but divides neither factor, while each of $\sqrt{5} - 1$ and $\sqrt{5} + 1$ divides $2 \cdot 2 = 4$ but does not divide 2. The ring $\mathbb{Z}[i]$ behaves better because it has a Euclidean division algorithm.

Corollary 27.3 If $N(\alpha)$ is a rational prime, then α is irreducible in $\mathbb{Z}[i]$.

Proof. If $\alpha = \beta\gamma$, then

$$N(\alpha) = N(\beta)N(\gamma).$$

Since $N(\alpha)$ is prime, one of $N(\beta)$ and $N(\gamma)$ is 1. By Proposition 26.5, one of β and γ is a unit. □

Theorem 27.4 The following elements are irreducible in $\mathbb{Z}[i]$.

1. The element $1 + i$.
2. Each rational prime $p \equiv 3 \pmod 4$.
3. Each $a + bi$ with $a^2 + b^2 = p$, where $p \equiv 1 \pmod 4$ is prime.

Proof. The element $1 + i$ has norm 2, so (1) follows from Corollary 27.3. Item (2) is exactly Theorem 26.7. Finally, if $a^2 + b^2 = p$, then $N(a + bi) = p$, so (3) again follows from Corollary 27.3. □

Lemma 27.5 (Divisibility lemma) Let $\alpha = a + bi \in \mathbb{Z}[i]$.

1. If $2 \mid N(\alpha)$, then $(1 + i) \mid \alpha$.
2. Let $p \equiv 1 \pmod 4$ be prime, and write

   $$p = u^2 + v^2 = (u + vi)(u - vi), \quad u, v > 0.$$

   If $p \mid N(\alpha)$, then $u + vi \mid \alpha$ or $u - vi \mid \alpha$.
3. Let $p \equiv 3 \pmod 4$ be prime. If $p \mid N(\alpha)$, then $p \mid \alpha$ in $\mathbb{Z}[i]$.

Proof. For (1), the congruence $2 \mid a^2 + b^2$ implies $a \equiv b \pmod 2$. Thus

$$\frac{\alpha}{1+i} = \frac{(a+bi)(1-i)}{2} = \frac{a+b}{2} + \frac{b-a}{2}i \in \mathbb{Z}[i].$$

For (3), suppose $p \mid a^2 + b^2$. We show that p divides both a and b. If $p \mid a$, then $p \mid b^2$, so $p \mid b$. Thus we may assume, for a contradiction, that $p \nmid a$. Then $p \nmid b$ as well, and

$$a^2 \equiv -b^2 \pmod{p}.$$

Multiplying by $(b^{-1})^2$ gives

$$\left(ab^{-1}\right)^2 \equiv -1 \pmod{p},$$

which contradicts $p \equiv 3 \pmod 4$ and Theorem 13.2. Hence $p \mid a$, and then $p \mid b$. Therefore $p \mid \alpha$.

For (2), first suppose that p divides both a and b. Then $\alpha = p\gamma$ for some $\gamma \in \mathbb{Z}[i]$, and since

$$p = (u + vi)(u - vi),$$

both $u + vi$ and $u - vi$ divide α.

Now suppose that p does not divide both a and b. We want to show that

$$\frac{\alpha}{u + vi} \in \mathbb{Z}[i] \qquad \text{or} \qquad \frac{\alpha}{u - vi} \in \mathbb{Z}[i].$$

Computing the two quotients gives

$$\frac{\alpha}{u + vi} = \frac{(a + bi)(u - vi)}{p} = \frac{au + bv}{p} + \frac{-av + bu}{p}i$$

and

$$\frac{\alpha}{u - vi} = \frac{(a + bi)(u + vi)}{p} = \frac{au - bv}{p} + \frac{av + bu}{p}i.$$

Thus it is enough to prove that either

$$p \mid au + bv \qquad \text{and} \qquad p \mid -av + bu,$$

or

$$p \mid au - bv \qquad \text{and} \qquad p \mid av + bu.$$

Write $a^2 + b^2 = pk$. Since $p = u^2 + v^2$, we have

$$\begin{aligned}(au + bv)(au - bv) &= a^2u^2 - b^2v^2 \\ &= a^2u^2 - b^2(p - u^2) \\ &= (a^2 + b^2)u^2 - b^2p \\ &= p(ku^2 - b^2),\end{aligned}$$

and

$$\begin{aligned}(-av+bu)(av+bu) &= b^2u^2 - a^2v^2 \\ &= b^2u^2 - a^2(p-u^2) \\ &= (a^2+b^2)u^2 - a^2p \\ &= p(ku^2 - a^2).\end{aligned}$$

Thus p divides each of these two products. Because p is prime, there are four possible combinations:

(a) $p \mid au+bv$ and $p \mid -av+bu$,
(b) $p \mid au+bv$ and $p \mid av+bu$,
(c) $p \mid au-bv$ and $p \mid -av+bu$,
(d) $p \mid au-bv$ and $p \mid av+bu$.

Cases (a) and (d) are exactly what we want. We show that the mixed cases cannot occur. Suppose case (b) holds. Then

$$p \mid b(au+bv) - a(av+bu) = (b^2-a^2)v.$$

Since $p = u^2+v^2$ with $u, v > 0$, we have $p \nmid v$, so $p \mid b^2-a^2$. Together with $p \mid a^2+b^2$, this gives $p \mid 2a^2$. Since p is odd, $p \mid a$, and then $p \mid b$, contradicting the assumption that p does not divide both a and b.

Case (c) is ruled out in the same way. If case (c) holds, then

$$p \mid b(au-bv) - a(-av+bu) = (a^2-b^2)v.$$

Again $p \nmid v$, so $p \mid a^2-b^2$. Combining this with $p \mid a^2+b^2$ gives $p \mid 2a^2$, and hence $p \mid a$ and $p \mid b$, the same contradiction. Therefore case (a) or case (d) must hold, and hence $u+vi \mid \alpha$ or $u-vi \mid \alpha$. □

Theorem 27.6 (Classification of Gaussian irreducibles) Every irreducible element of $\mathbb{Z}[i]$ is associated to exactly one of the following types:

1. $1+i$.
2. A prime p in $\mathbb{Z}$ with $p \equiv 3 \pmod 4$;
3. An element $a+bi$ with $a^2+b^2 = p$, where $p \equiv 1 \pmod 4$ is prime in $\mathbb{Z}$.

Proof. The elements listed are irreducible by Theorem 27.4. Conversely, let α be irreducible. Choose a rational prime p dividing $N(\alpha)$.

If $p = 2$, then Lemma 27.5(1) gives $(1+i) \mid \alpha$. Since α is irreducible, α is associated to $1+i$.

If $p \equiv 3 \pmod 4$, then Lemma 27.5(3) gives $p \mid \alpha$, so α is associated to p.

If $p \equiv 1 \pmod 4$, then Theorem 17.5 gives $p = a^2 + b^2$ with $a, b > 0$, and Lemma 27.5(2) gives $a + bi \mid \alpha$ or $a - bi \mid \alpha$. Again irreducibility forces α to be associated to one of these factors. □

Lecture 28 — Friday, November 20, 2015

Theorem 28.1 (Division algorithm in $\mathbb{Z}[i]$) Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. Then there are $\gamma, \rho \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \rho \qquad \text{and} \qquad N(\rho) < N(\beta).$$

Proof. Write

$$\frac{\alpha}{\beta} = a + bi \quad (a, b \in \mathbb{R}).$$

Choose integers c, d with

$$|a - c| \leq \frac{1}{2} \qquad \text{and} \qquad |b - d| \leq \frac{1}{2},$$

and set $\gamma = c + di$. Let $\rho = \alpha - \beta\gamma$. Then

$$\frac{\rho}{\beta} = \frac{\alpha}{\beta} - \gamma = (a - c) + (b - d)i,$$

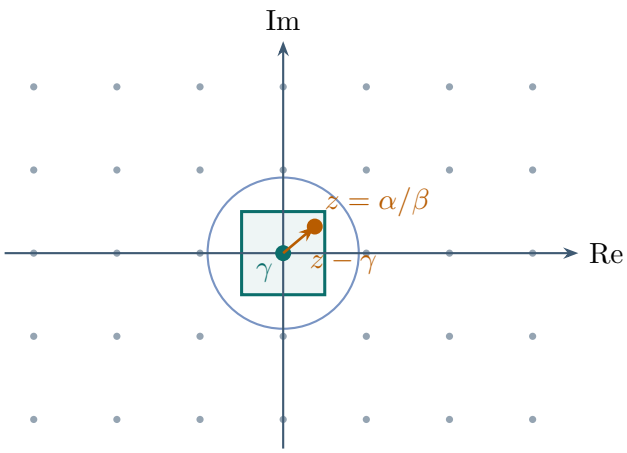
so

$$N\left(\frac{\rho}{\beta}\right) = (a-c)^2 + (b-d)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Multiplying by $N(\beta)$ gives $N(\rho) < N(\beta)$. □

The rounding step is geometric. In Figure 9, the complex quotient $z = \alpha/\beta$ lies in the half-unit square around a nearest Gaussian integer γ; that square lies inside the unit circle, so $N(z - \gamma) < 1$ and hence $N(\rho) < N(\beta)$.

Remark 28.2 The quotient γ and remainder ρ are not necessarily unique.



rounding real and imaginary parts puts the normalized remainder inside the unit disk

FIGURE 9

Example 28.3 Let $\alpha = 28 + 41i$ and $\beta = 7 + 3i$. Then

$$\frac{\alpha}{\beta} = \frac{(28+41i)(7-3i)}{(7+3i)(7-3i)} = \frac{319+203i}{58} = \frac{11}{2} + \frac{7}{2}i.$$

There is more than one nearest Gaussian integer. If $\gamma_1 = 5 + 3i$, then

$$\rho_1 = \alpha - \beta\gamma_1 = (28+41i) - (7+3i)(5+3i) = 2 + 5i,$$

and if $\gamma_2 = 6 + 3i$, then

$$\rho_2 = \alpha - \beta\gamma_2 = (28+41i) - (7+3i)(6+3i) = -5 + 2i.$$

Both choices satisfy

$$N(\rho_1) = N(\rho_2) = 29 < 58 = N(\beta).$$

Theorem 28.4 (Common divisor property in $\mathbb{Z}[i]$) Let $\alpha, \beta \in \mathbb{Z}[i]$, not both zero. Let

$$S = \{A\alpha + B\beta : A, B \in \mathbb{Z}[i]\}.$$

Choose a nonzero $g \in S$ with minimal positive norm among the nonzero elements of S. Then g divides both α and β. Moreover, every common divisor of α and β divides g.

Remark 28.5 The element g is not necessarily unique, since multiplying by a unit gives another greatest common divisor.

Proof. By Theorem 28.1, write

$$\alpha = \gamma g + \rho \qquad \text{with} \qquad N(\rho) < N(g).$$

Since $g = A_0\alpha + B_0\beta$ for some $A_0, B_0 \in \mathbb{Z}[i]$, we have

$$\rho = \alpha - \gamma g = (1 - \gamma A_0)\alpha - \gamma B_0 \beta \in S.$$

The minimality of $N(g)$ forces $\rho = 0$, so $g \mid \alpha$. The same argument gives $g \mid \beta$.

If δ is any common divisor of α and β, then δ divides every element of S, and in particular $\delta \mid g$. □

Lecture 29 — Monday, November 23, 2015

Definition 29.1 An element $g \in \mathbb{Z}[i]$ is a **greatest common divisor** of α and β if g is a common divisor of α and β, and every common divisor of α and β divides g.

Corollary 29.2 Every pair of Gaussian integers, not both zero, has a greatest common divisor.

Proof. This is exactly Theorem 28.4. □

Theorem 29.3 (Irreducibles are prime in $\mathbb{Z}[i]$) Every irreducible element of $\mathbb{Z}[i]$ is prime.

Proof. Let π be irreducible, and suppose $\pi \mid \alpha\beta$. We prove that $\pi \mid \alpha$ or $\pi \mid \beta$.

Apply the common divisor property to π and α, and let g be the resulting greatest common divisor.

Since $g \mid \pi$ and π is irreducible, either g is associated to π or g is a unit.

In the first case, $\pi \mid g$. Since $g \mid \alpha$, we get $\pi \mid \alpha$.

In the second case, g is a unit. Since $g = A\pi + B\alpha$ for some $A, B \in \mathbb{Z}[i]$, multiplying by g^{-1} gives

$$A'\pi + B'\alpha = 1$$

for some $A', B' \in \mathbb{Z}[i]$. Multiplying by β gives

$$A'\pi\beta + B'\alpha\beta = \beta.$$

Both terms on the left are divisible by π, so $\pi \mid \beta$. □

Definition 29.4 A nonzero Gaussian integer $\alpha = x + yi$ is **normalized** if $x > 0$ and $y \geq 0$. Every nonzero Gaussian integer is associated to exactly one normalized element.

Theorem 29.5 (Unique factorization in $\mathbb{Z}[i]$) Every nonzero Gaussian integer α can be written in the form

$$\alpha = u\pi_1^{e_1} \cdots \pi_r^{e_r},$$

where u is a unit, the π_j are distinct normalized Gaussian primes, and the e_j are positive integers. This factorization is unique up to the order of the factors.

Proof. We first prove existence by induction on $N(\alpha)$. If $N(\alpha) = 1$, then α is a unit by Proposition 26.5. Suppose $N(\alpha) = k > 1$, and assume that every Gaussian integer with norm less than k has such a factorization.

If α is irreducible, then it is prime by Theorem 29.3. Multiplying by a unit makes it normalized, so this already gives the desired factorization. If α is reducible, write

$$\alpha = \beta\gamma$$

where neither β nor γ is a unit. Then

$$1 < N(\beta) < N(\alpha) \qquad \text{and} \qquad 1 < N(\gamma) < N(\alpha),$$

because

$$N(\beta) = \frac{N(\alpha)}{N(\gamma)} \qquad \text{and} \qquad N(\gamma) = \frac{N(\alpha)}{N(\beta)}.$$

By the induction hypothesis, both β and γ factor into a unit times normalized Gaussian primes. Multiplying these two factorizations gives the desired factorization of α.

For uniqueness, suppose

$$\alpha = u\pi_1^{e_1} \cdots \pi_r^{e_r} = v\delta_1^{f_1} \cdots \delta_s^{f_s}$$

are two factorizations into normalized Gaussian primes. We again argue by induction on $N(\alpha)$. If $N(\alpha) = 1$, then α is a unit and there are no prime factors.

Now assume $N(\alpha) > 1$. Then some e_i is nonzero; say $e_1 > 0$. Since π_1 is prime and

$$\pi_1 \mid v\delta_1^{f_1} \cdots \delta_s^{f_s},$$

the prime π_1 divides some δ_j. Because δ_j is irreducible, π_1 and δ_j are associates. Both are normalized, so they are equal. Reordering the second factorization, assume $\delta_1 = \pi_1$.

Set

$$\beta = \frac{\alpha}{\pi_1}.$$

Then $N(\beta) < N(\alpha)$, and the two induced factorizations of β are unique by the induction hypothesis. Therefore the remaining normalized primes and exponents agree, and the unit factor agrees as well. This proves uniqueness. □

Lecture 30 — Wednesday, November 25, 2015

Applications of Gaussian Integers

Question 30.1 How many ways are there to write a positive integer N as a sum of two squares?

Definition 30.2 For a positive integer N, define

$$R(N) = \#\{(a, b) \in \mathbb{Z}^2 : N = a^2 + b^2\}.$$

Thus signs and order are counted.

Remark 30.3 The identity

$$N = a^2 + b^2 = (a + bi)(a - bi)$$

shows that counting representations of N as a sum of two squares is the same as counting Gaussian integers $\alpha = a + bi$ with

$$N(\alpha) = N.$$

Example 30.4 We have

$$R(2) = 4,$$

corresponding to $(\pm 1, \pm 1)$. Also

$$R(5) = 8,$$

corresponding to $(\pm 1, \pm 2)$ and $(\pm 2, \pm 1)$. For 4, the only representations are

$$4 = (\pm 2)^2 + 0^2 = 0^2 + (\pm 2)^2,$$

so $R(4) = 4$. Finally,

$$20 = (\pm 4)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 4)^2,$$

so $R(20) = 8$.

Example 30.5 The representation count for 20 can be seen directly in $\mathbb{Z}[i]$:

$$20 = 2^2 \cdot 5 = (\text{unit}) \cdot (1 + i)^4 (2 + i)(2 - i).$$

Half of the factor $(1+i)^4$, namely $(1+i)^2$, is forced into $a+bi$ up to a unit, while the factor $2 + i$ may be placed in either $a + bi$ or $a - bi$. There are four choices for the unit and two choices for this conjugate pair, giving 8 representations.

Recall that N can be written as a sum of two squares if and only if $N = 2^e p_1^{t_1} \cdots p_l^{t_l} M^2$, where the p_i are distinct primes congruent to 1 modulo 4, and M is a product of primes congruent to 3 modulo 4. Suppose $M = q_1^{s_1} \cdots q_r^{s_r}$, so that

$$N = 2^e p_1^{t_1} \cdots p_l^{t_l} \, (q_1^{s_1} \cdots q_r^{s_r})^2 = (1 + i)^e (1 - i)^e (\pi_1 \overline{\pi_1})^{t_1} \cdots (\pi_l \overline{\pi_l})^{t_l} (q_1^{s_1} \cdots q_r^{s_r})^2.$$

How many ways can we make this arrangement?

Lecture 31 — Friday, November 27, 2015

Theorem 31.1 (Representation count by factorization) Let

$$N = 2^e p_1^{t_1} \cdots p_n^{t_n} q_1^{s_1} \cdots q_r^{s_r},$$

where the p_i are distinct primes congruent to 1 modulo 4, and the q_j are distinct primes congruent to 3 modulo 4. Then

$$R(N) = \begin{cases} 4(t_1+1)\cdots(t_n+1), & \text{if all } s_j \text{ are even,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. If $N = a^2 + b^2$, then

$$N = (a+bi)(a-bi).$$

In this factorization, a rational prime $q_j \equiv 3 \pmod 4$ remains a Gaussian prime and is equal to its own conjugate. Thus the exponent of q_j in N must be split equally between $a+bi$ and $a-bi$. If one of the s_j is odd, this is impossible, so $R(N) = 0$.

Assume all s_j are even. For each $p_i \equiv 1 \pmod 4$, choose a Gaussian prime π_i such that

$$p_i = \pi_i \overline{\pi_i}.$$

Using $2 = (\text{unit}) \cdot (1+i)^2$, the factorization of N in $\mathbb{Z}[i]$ has the form

$$N = (\text{unit}) \cdot (1+i)^{2e} \prod_{i=1}^{n} (\pi_i \overline{\pi_i})^{t_i} \prod_{j=1}^{r} q_j^{s_j}.$$

The factor $(1+i)^{2e}$ is forced to contribute $(1+i)^e$ to $a+bi$, up to a unit. Each $q_j^{s_j}$ is also forced to contribute $q_j^{s_j/2}$ to $a+bi$. The only choices come from the conjugate pairs above $p_i \equiv 1 \pmod 4$: if r_i copies of π_i go into $a+bi$, then the remaining $t_i - r_i$ copies of $\overline{\pi_i}$ go into $a+bi$. Therefore, by unique factorization in Theorem 29.5, the Gaussian integer $a+bi$ must be

$$a+bi = u(1+i)^e \prod_{i=1}^{n} \pi_i^{r_i} \overline{\pi_i}^{t_i - r_i} \prod_{j=1}^{r} q_j^{s_j/2},$$

where u is one of the four units and $0 \le r_i \le t_i$ for each i.

Conversely, every such choice gives a Gaussian integer of norm N. There are four choices for u and $t_i + 1$ choices for each r_i, so the number of choices is

$$4(t_1 + 1) \cdots (t_n + 1).$$

□

Theorem 31.2 (Legendre's theorem on two squares) Let $D_1(N)$ be the number of positive divisors of N that are congruent to 1 modulo 4, and let $D_3(N)$ be the number of positive divisors of N that are congruent to 3 modulo 4. Then

$$R(N) = 4\big(D_1(N) - D_3(N)\big).$$

Proof. Use the same prime factorization as in Theorem 31.1. Divisors divisible by 2 do not contribute to either $D_1(N)$ or $D_3(N)$. A divisor not divisible by 2 has the form

$$d = p_1^{r_1} \cdots p_n^{r_n} q_1^{\ell_1} \cdots q_r^{\ell_r}.$$

Since each $p_i \equiv 1 \pmod 4$ and each $q_j \equiv 3 \pmod 4$, the residue class of d modulo 4 is determined by the parity of

$$\ell_1 + \cdots + \ell_r.$$

Therefore

$$D_1(N) - D_3(N) = \prod_{i=1}^{n} (t_i + 1) \prod_{j=1}^{r} (1 - 1 + 1 - \cdots + (-1)^{s_j}).$$

The second product is 1 when every s_j is even and 0 otherwise. Comparing with Theorem 31.1 proves the formula. □

That about wraps up the easy part of number theory.

5. Elliptic Curves

Elliptic Curves

We introduce elliptic curves by first revisiting the unit circle. Integer solutions of

$$a^2 + b^2 = c^2$$

are the Pythagorean triples studied earlier. In the primitive case, after interchanging a and b if necessary, they are obtained from odd coprime integers $s > t$ by

$$a = st, \qquad b = \frac{s^2 - t^2}{2}, \qquad \text{and} \qquad c = \frac{s^2 + t^2}{2}.$$

Dividing $a^2 + b^2 = c^2$ by c^2 converts the same problem into the problem of finding rational points on

$$x^2 + y^2 = 1.$$

The point $O = (-1, 0)$ is already rational. If $P = (x, y) \neq O$ is another rational point on the circle, then the line through O and P has rational slope

$$m = \frac{y}{x + 1}.$$

Figure 10 shows the secant construction geometrically.

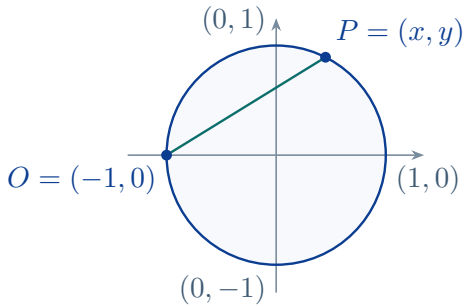


FIGURE 10

Conversely, a line through O with rational slope m has equation

$$y = m(x + 1).$$

Substituting into $x^2 + y^2 = 1$ gives

$$(1 + m^2)x^2 + 2m^2x + (m^2 - 1) = 0.$$

One root is $x = -1$, so the other is

$$x = \frac{1 - m^2}{1 + m^2} \qquad \text{and} \qquad y = \frac{2m}{1 + m^2}.$$

Thus every rational slope gives a rational point on the circle. Writing $m = v/u$ with $\gcd(u, v) = 1$ gives

$$x = \frac{u^2 - v^2}{u^2 + v^2} \qquad \text{and} \qquad y = \frac{2uv}{u^2 + v^2},$$

and hence the Pythagorean triple

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2.$$

Lecture 32 — Monday, November 30, 2015

Definition 32.1 An **elliptic curve** over $\mathbb{Q}$ is a nonsingular curve of the form

$$E : y^2 = x^3 + Ax^2 + Bx + C, \quad A, B, C \in \mathbb{Q},$$

together with a point at infinity, denoted $\mathcal{O}$. Here "nonsingular" means that the cubic on the right has no repeated root.

The central problem is to understand the rational points on E, namely points $(x, y) \in \mathbb{Q}^2$ satisfying the equation, together with $\mathcal{O}$.

Example 32.2 Let

$$E : y^2 = x^3 + 17.$$

The point $P = (-2, 3)$ lies on E. The line through P with slope 1 is

$$y - 3 = x + 2, \qquad \text{so} \qquad y = x + 5.$$

Substituting into the equation of E gives

$$(x + 5)^2 = x^3 + 17,$$

or

$$x^3 - x^2 - 10x - 8 = 0.$$

Since $x = -2$ is one root,

$$x^3 - x^2 - 10x - 8 = (x + 2)(x - 4)(x + 1).$$

Thus the same line also gives the rational points

$$(-1, 4) \qquad \text{and} \qquad (4, 9).$$

If instead we use the line of slope 3 through P, then $y = 3x + 9$, and substitution gives

$$x^3 - 9x^2 - 54x - 64 = (x + 2)(x^2 - 11x - 32).$$

The quadratic factor has discriminant 249, so this line gives no additional rational point.

Example 32.3 Suppose we already have insider information in the form of two rational points on $E : y^2 = x^3 + 17$:

$$P = (-2, 3) \qquad \text{and} \qquad Q = (2, 5).$$

The line through them has slope $1/2$, so its equation is

$$y = \frac{x}{2} + 4.$$

Substituting into E gives

$$4x^3 - x^2 - 16x + 4 = 0.$$

The roots are -2, 2, and $1/4$, so the third intersection point is

$$R = \left(\frac{1}{4}, \frac{33}{8}\right).$$

Definition 32.4 Let P and Q be rational points on an elliptic curve E. The line through P and Q intersects E in a third point R, counted with multiplicity; if $P = Q$, use the tangent line at P. The **elliptic curve sum** is defined by reflecting this third point across the x-axis:

$$P \oplus Q = -R.$$

The point at infinity $\mathcal{O}$ is the identity element, and vertical lines give $P \oplus (-P) = \mathcal{O}$.

Proposition 32.5 With the operation $\oplus$, the rational points on an elliptic curve form an abelian group.

Commutativity is visible from the construction. Associativity is much deeper and is usually proved using projective geometry or algebraic geometry.

Theorem 32.6 (Mordell's theorem) For an elliptic curve E over $\mathbb{Q}$, the group $E(\mathbb{Q})$ of rational points is finitely generated. Equivalently, there are rational points $P_1, \dots, P_k$ such that every rational point on E is a finite sum of these points and their inverses.

The proof of Theorem 32.6 is very, *very* hard and well beyond the scope of this course, but the theorem explains why the chord-and-tangent construction is not merely a way to find examples: in principle, finitely many rational points generate all of them.

Definition 32.7 A rational point P on an elliptic curve is a **torsion point** if there is an integer $k \geq 1$ such that

$$\underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ times}} = \mathcal{O}.$$

Theorem 32.8 Let $E : y^2 = x^3 + Ax + B$ be a nonsingular elliptic curve with $A, B \in \mathbb{Z}$.

1. (**Nagell–Lutz theorem**) If $P = (x, y) \in E(\mathbb{Q})$ is a finite torsion point, then $x, y \in \mathbb{Z}$, and either $y = 0$ or y^2 divides $4A^3 + 27B^2$.
2. (**Mazur's theorem**) The rational torsion subgroup of E is either cyclic of order n for $1 \leq n \leq 10$ or $n = 12$, or isomorphic to

$$\mathbb{Z}_2 \times \mathbb{Z}_{2m} \qquad \text{for some } 1 \leq m \leq 4.$$

We do not prove these results here; they belong to a full course in elliptic curves.

Appendix: Lecture and Tutorial Index