Lecture notes
Number Theory and Cryptography

Matt Kerr

Contents

Introduction

Number theory has its roots in the study of the properties of the natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

and various "extensions" thereof, beginning with the integers

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

and rationals

$$\mathbb{Q} = \left\{ \tfrac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

This leads directly to the first two parts of this course, of which the following may serve as a brief outline.

* * *

I. Divisibility.

- Euclidean algorithm and greatest common divisors.
- Primes and the Fundamental Theorem of Algebra.
- Results and conjectures concerning primes: Euclid's theorem; the Riemann zeta function; arithmetic progressions.

II. Congruences.

- Modular (clock) arithmetic: $a^{p-1} \equiv 1 \pmod{p}$ and its generalizations.
- Chinese remainder theorem: given $x \underset{(p)}{\equiv} a$ and $x \underset{(q)}{\equiv} b$, find $x \pmod{pq}$.
- A first view of primality testing and factorization.
- Groups, rings and fields (especially finite abelian groups and finite fields).

- Primitive roots modulo a prime: e.g. mod 7, $3 \cdot 3 \underset{(7)}{\equiv} 2$, so 2 has a square root!
- Quadratic reciprocity: e.g., if 37 is a square modulo 11, this allows you to decide without computation whether 11 is a square modulo 37 (which it is).

III. Cryptography (a first look).

- Simple cryptosystems and symmetric ciphers.
- Public key cryptography: answers the question "How can two parties communicate securely over an *insecure* channel without *first* privately exchanging some kind of 'key' to each others' messages?" They need a *trapdoor function* f that can be used to encode information easily but hard to invert without knowing "extra information".
- Diffie-Hellman key exchange (based on difficulty of solving $a^x \underset{(p)}{\equiv} b$ for x) and the discrete log problem.
- RSA cryptosystem: this is based on the difficulty of solving $x^e \underset{(N)}{\equiv} c$ when $N = pq$.
- Introduction to GP-PARI (computer package for number theory).
- Pollard $p-1$ factorization method: this helps us understand when RSA could be potentially broken.

IV. Diophantine equations.

- This is the part of number theory that studies polynomial equations in integers or rationals. A famous example is the insolubility of $x^m + y^m = z^m$ (apart from the "trivial" solution $(0,0,0)$) for $m \geq 3$, known as *Fermat's last theorem* (proved by Andrew Wiles).
- Pythagoras's theorem and Fibonacci numbers.
- Pell's equation ($x^2 - dy^2 = \pm 1$) and quadratic number fields.

- Cubic equations and the group law for elliptic curves.[1]

V. Elliptic curve cryptography.

- The security of using elliptic curves for cryptography rests on the difficulty of solving an analogue of the discrete log problem.
- We can also use the group law on an elliptic curve to factor large numbers (Lenstra's algorithm).
- A deeper, more flexible sort of cryptosystem can be obtained from the "Weil pairing" on m-torsion points of an elliptic curve.

V. Algebraic numbers.

- These appeared under the guise of "ideal numbers" in the mid-19th century. Easy examples include $a + b\sqrt{-1}$, where $a, b \in \mathbb{Z}$.
- Cyclotomic fields and an "easy" case of Fermat's last theorem.
- Failure of unique factorization in general.
- Irrationality and Galois groups.
- Ideals and class groups.
- Fermat's last theorem (less easy case, still far from the whole thing).

* * *

Now the natural numbers have a well-defined notion of order, which leads to the following property:

[1]Confusing terminology: these are not ellipses, which are defined by a quadratic equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, but rather are defined by cubic (and sometimes quartic) equations such as $y^2 = x^3 + \alpha x + \beta$ (or $y^2 = (1 - x^2)(1 - \kappa^2 x^2)$). They are called "elliptic" for the arcane historical reason that a related "elliptic integral" $\int_0^1 \frac{1-\kappa^2 x^2}{\sqrt{(1-x^2)(1-\kappa^2 x^2)}} dx$ arises in the course of determining the arclength of an ellipse.

THEOREM 1 (Principle of the least element). *Let $\mathcal{S} \subset \mathbb{N}$ be a nonempty subset. Then $\mathcal{S}$ has a least element, i.e. there exists $s \in \mathcal{S}$ such that for every $x \in \mathcal{S}$, $s \leq x$.*

(This also applies to $\mathbb{N} \cup \{0\}$.) Theorem 1 implies the well-known

THEOREM 2 (Principle of mathematical induction). *Let $S(x)$ be a statement about any $x \in \mathbb{N}$. Suppose that*

(i) *$S(1)$ is true and*
(ii) *$S(x)$ true $(\forall x < n) \implies S(n)$ true.*

Them $S(x)$ is true for all $x \in \mathbb{N}$.

PROOF THAT THEOREM 1 $\implies$ THEOREM 2. Assume that (i) and (ii) hold, and *suppose that*

$$\mathscr{F} := \{x \in \mathbb{N} \mid S(x) \text{ false}\}$$

is nonempty. Then $\mathscr{F}$ has a least element f, by Theorem 1. Hence, for any $x < f$, we have $x \notin \mathscr{F}$ — i.e. $S(x)$ is true. Now consider the following two cases:

- $\underline{f = 1}$: impossible, as it contradicts (i).
- $\underline{f > 1}$: by (ii), $S(f)$ is then true, contradicting $f \in \mathscr{F}$.

Therefore our supposition was absurd, and $\mathscr{F}$ is empty. □

Part 1

Primes and divisibility

CHAPTER 1

The Euclidean Algorithm

We begin our discussion with the **division algorithm**:

PROPOSITION 3. *Given $a, b \in \mathbb{N}$, there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = b \cdot q + r \ \text{ with } \ 0 \leq r < b.$$

Of course, the "algorithm" isn't in the formal statement, but in how we produce q and r.

EXAMPLE 4. Suppose $a = 313$ and $b = 9$. In grade school, you learned to write

$$\begin{array}{r} 34 \\ \hline 9\,\big)\,313 \\ 27 \\ \hline 43 \\ 36 \\ \hline 7 \end{array}$$

which yields

$$313 = 9 \cdot \underbrace{34}_{q} + \underbrace{7}_{r}.$$

The algorithm is simply long division with remainder.

PROOF OF PROPOSITION 3. For the "existence" part, let

$$\mathcal{S} := \{a - bk \mid k \in \mathbb{Z},\ a - bk \geq 0\} \subseteq \mathbb{N} \cup \{0\}.$$

Since $a \in \mathcal{S}$, $\mathcal{S} \neq \emptyset$. Let r be the least element of $\mathcal{S}$. Then $r = a - bq \geq 0$ for some $q \in \mathbb{Z}$. If $r \geq b$ then $\mathcal{S}$ contains $r - b = a - b(q+1)$, contradicting minimality of r. So $r < b$.

To see the uniqueness, write

$$bq' + r' = a = bq + r,$$

with $0 \leq r, r' < b$. This yields

$$r = b(q' - q) + r',$$

and if we had $q' > q$, then $q' \geq q + 1$ would imply $r \geq b + r' \geq b + 0 = b$, a contradiction. Symmetrically, one argues that $q > q'$ is impossible. Therefore $q = q'$ and then also $r = r'$. □

Next, we turn to **divisibility** and the **GCD** (= greatest common divisor).

DEFINITION 5. Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Then

$$b \mid a \quad \underset{\text{defn.}}{\iff} \quad \exists\, c \in \mathbb{Z} \text{ such that } a = bc.$$

(We say that "b divides a".)

Here are some basic examples:

- everything divides 0;
- $2|a \iff a$ is even;
- $b|a \iff r = 0$ in the division algorithm.

and some basic properties:

(i) $a|b$ and $b|c \implies a|c$

(ii) $a|b, c \implies a|bx + cy$ for all $x, y \in \mathbb{Z}$ (e.g. $b + c$, $b - c$)

(iii) $a|b$ and $b|a \implies a = \pm b$.

PROOF OF (III). Given $b = ad$, $a = bc$ (and $a, b \neq 0$), we have $a = adc \implies dc = 1 \implies d = \pm 1 = c$. □

For any $a, b \in \mathbb{Z}$, not both 0, let

$$\mathcal{S}(a, b) := \{d \in \mathbb{N} \mid d|a, b\}.$$

DEFINITION 6. The *GCD of a and b* is

$$(a, b) := \text{ the biggest element of } \mathcal{S}(a, b).$$

(Of course, you need only check integers less than or equal to the smallest of $|a|$ and $|b|$.) We say that a and b are *relatively prime* if $(a, b) = 1$.

Again, here are some simple examples:

- $(4,-6)=2$
- $(0,7)=7$
- $(12,7)=1$

and some properties:

(iv) $(0,b)=b=(b,b)$
(v) $(a,b)=(b,a)=(a,-b)$
(vi) $(b,a-mb)=(a,b)$ for every $m\in\mathbb{Z}$.

PROOF OF (VI). Let $d|a,b$. Then $d|a-mb$. Conversely, if $d|b,a-mb$, then $d|mb+(a-mb)=a$. So $\mathcal{S}(a,b)=\mathcal{S}(b,a-mb)$ and they have identical largest elements. □

Property (vi) has the key consequence:

LEMMA 7. *Say $a=bq+r$ in the division algorithm. Then*

$$(a,b)=(b,r).$$

PROOF. Write $r=a-bq$, and use (vi). □

EXAMPLE 8. How do we use this to find a GCD, like $(345,92)$? By applying it in concert with the division algorithm: starting with $a=345$ and $b=92$, we have

$$\left\{\begin{array}{rcl}345&=&92\cdot 3+69\\ a&=&b\cdot q_1+r_1\end{array}\right.\Longrightarrow\left\{\begin{array}{rcl}(345,92)&=&(92,69)\\ (a,b)&=&(b,r_1)\end{array}\right.$$

$$\left\{\begin{array}{rcl}92&=&69\cdot 1+23\\ b&=&r_1\cdot q_2+r_2\end{array}\right.\Longrightarrow\left\{\begin{array}{rcl}(92,69)&=&(69,23)\\ (b,r_1)&=&(r_1,r_2)\end{array}\right.$$

$$\left\{\begin{array}{rcl}69&=&23\cdot 3+0\\ r_1&=&r_2\cdot q_3+r_3\end{array}\right.\Longrightarrow\left\{\begin{array}{rcll}(69,23)&=&(23,0)&=23\\ (r_1,r_2)&=&(r_2,r_3)&\end{array}\right.\quad.$$

So $(345,92)=23$.

THEOREM 9 (**Euclidean Algorithm**). *Given $a,b\in\mathbb{N}$, (a,b) may be computed by repeated application of the Division Algorithm. That is,*

writing

$$\begin{array}{rcl} a = bq_1 + r_1 & , & 0 \leq r_1 < b, \\ b = r_1q_2 + r_2 & , & 0 \leq r_2 < r_1, \\ r_1 = r_2q_3 + r_3 & , & 0 \leq r_3 < r_2, \\ \vdots & & \vdots \end{array}$$

we eventually reach

$$\begin{array}{cc} \vdots & \vdots \\ r_{n-1} = r_nq_{n+1} + r_{n+1} \quad \textit{with} & r_{n+1} = 0, \end{array}$$

and then $(a, b) = r_n$.

PROOF. There are two statements here: *first*, that the algorithm terminates after finitely many steps. But we have $b > r_1 > r_2 > \cdots \geq 0$ (as a byproduct of Proposition 3), which clearly cannot continue indefinitely, so that indeed we must have $r_{n+1} = 0$ for some n.

Second, the theorem claims that $(a, b) = r_n$. To see this, we just use Lemma 7 to write

$$(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_n, r_{n+1}) = (r_n, 0) = r_n.$$

□

Now returning to Example 8, the first two equations yield the following "bonus"

$$\begin{array}{rcl} 23 & = & 92 - 69 \cdot 1 \\ & = & 92 - (345 - 92 \cdot 3) \cdot 1 \\ & = & 4 \cdot 92 + (-1) \cdot 345 \end{array} \qquad \begin{array}{rcl} r_2 & = & b - r_1q_2 \\ & = & b - (a - bq_1)q_2 \\ & = & (1 + q_1q_2)b + (-q_2)a \end{array}$$

expressing the GCD as an integer linear combination of a and b. This is a general fact: let a, b be integers, not both zero.

THEOREM 10. *There exist* $x, y \in \mathbb{Z}$ *such that* $(a, b) = ax + by$.

PROOF. In the Euclidean algorithm, (a, b) appears as the last nonzero remainder r_n. we show by induction that all the remainders are integer linear combinations of a and b.

For $n = 1$, we have $r_1 = a + (-q_1)b$. Now assume that $r_j = ax_j + by_j$ ($x_j, y_j \in \mathbb{Z}$) for $j = 1, \ldots, k-1$. To check that this is true for $j = k$, write $r_{k-2} = r_{k-1}q_k + r_k \implies$

$$r_k = r_{k-2} + (-q_k)r_{k-1} = (x_{k-2}a + y_{k-2}b) + (-q_k)(x_{k-1}a + y_{k-1}b)$$
$$= \underbrace{(x_{k-2} - q_k x_{k-1})}_{=:x_k} a + \underbrace{(y_{k-2} - q_k y_{k-1})}_{=:y_k} b.$$

□

COROLLARY 11. *(a, b) is the least element of*

$$\mathcal{S} := \{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}.$$

PROOF. Given any $\mu = ax_0 + by_0 \in \mathcal{S}$, $g := (a, b)$ ($\in \mathcal{S}$ by Theorem 10). Then $g|a, b \implies g|\mu \implies \frac{\mu}{g} \in \mathbb{N} \implies g \leq \mu$. □

COROLLARY 12.

(i) $(ma, mb) = m(a, b)$ *for any* $m \in \mathbb{N}$

(ii) $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$ *if* $d|a, b$ *and* $d \in \mathbb{N}$.

PROOF. (ii) follows from (i), and (i) follows from the observation that the least positive number of the form $max + mby$ is m times the least positive number of the form $ax + by$. □

By part (ii), writing $g := (a, b)$, $(\frac{a}{g}, \frac{b}{g}) = 1$.

COROLLARY 13.

(i) *If a, b are relatively prime to m, then so is ab.*

(ii) *If $(b, m) = 1$ and $m|ab$, then $m|a$.*

PROOF. For (i), observe that there exist $x, y, z, w \in \mathbb{Z}$ such that $bz + mw = 1 = ax + my$. Hence

$$1 = (ax + my)(bz + mw) = ab(xz) + m(ybz + axw + myw),$$

and we are done by Corollary 11.

To see (ii), write $a = a \cdot 1 = a(b, m) = (ab, am) = m(\frac{ab}{m}, a)$. □

DEFINITION 14. The **LCM** (= *least common multiple*) $[a,b]$ is the least element of $\mathcal{S}' := \{n \in \mathbb{N} \mid a,b|n\}$.

COROLLARY 15. *We have* $[a,b](a,b) = ab$.

PROOF. Set $g := (a,b)$. Clearly $\frac{ab}{g} = a(\frac{b}{g}) = b(\frac{a}{g}) \in \mathcal{S}'$. But is this number "least" among elements of $\mathcal{S}'$?

If $a,b|N$ (i.e. $N \in \mathcal{S}'$) then $N = Ma$ and $\frac{b}{g}|\frac{N}{g} = M\frac{a}{g}$. By Corollary 13(ii), $(\frac{a}{g},\frac{b}{g}) = 1 \implies \frac{b}{g}|M \implies \frac{ab}{g}|Ma = N \implies N \geq \frac{ab}{g}$. □

As useful as Theorem 10 is, the method indicated in its proof yields awful formulas that require remembering all the $\{q_i\}$: for example, if $r_3 = (a,b)$, then

$$x = 1 + q_2q_3 \text{ and } y = -(q_1 + q_3 + q_1q_2q_3).$$

A better approach is to perform the Division Algorithm *on equations*: start with

	r_i		x_i		y_i	
$\begin{cases} \\ \\ \end{cases}$	345	$=$	$345 \cdot 1$	$+$	$92 \cdot 0$	$\mathbf{E_{-1(=i)}}$
	92	$=$	$345 \cdot 0$	$+$	$92 \cdot 1$	$\mathbf{E_0}$

Now perform the Division Algorithm: subtract $3 \cdot \mathbf{E_0}$ from $\mathbf{E_{-1}}$ to get

$$69 = 345 \cdot 1 + 92 \cdot (-3) \qquad \mathbf{E_1},$$

then $1 \cdot \mathbf{E_1}$ from $\mathbf{E_0}$ to get

$$23 = 345 \cdot (-1) + 92 \cdot 4 \qquad \mathbf{E_2}.$$

(We stop here becaue $\mathbf{E_3}$ would have 0 on the left-hand side.) The point is that we have

$$r_{i+1} = r_{i-1} - q_{i+1}r_i$$

as before, but also

$$\begin{cases} x_{i+1} = x_{i-1} - q_{i+1}x_i \\ y_{i+1} = y_{i-1} - q_{i+1}y_i \end{cases}$$

by virtue of carrying the operations through to the whole equation. The result is the following, which uses almost no memory on a computer:

THEOREM 16 (Algorithm for computing x and y). *Begin with the picture*

"r"	a	b	
"x"	1	0	
"y"	0	1	

and apply the Euclidean Algorithm to the top row, carrying operations through to the entire column at each stage:

		q_1	q_2	q_3	$\cdots$	q_n	q_{n+1}
a	b	r_1	r_2	r_3	$\cdots$	r_n	0
1	0	x_1	x_2	x_3	$\cdots$	x_b	$-$
0	1	y_1	y_2	y_3	$\cdots$	y_n	$-$
column:	-1	0	1	2	3	$\cdots$	n	$n+1$

—- *that is,* $col_{i+1} = col_{i-1} - q_{i+1}col_i$. *Then* $x_n a + y_n b = r_n = (a, b)$.

PROOF. At each stage, we have $r_k = x_k a + y_k b$, so the conclusion is clear. □

For computer (or human[1]) implementation of the Euclidean Algorithm, one problem remains: how large can $n+1$ (the number of steps) be?

THEOREM 17. *Assume* $a \geq b$. *We have* $n \leq 2\log_2(b)$.

LEMMA 18. $r_{i+2} < \frac{1}{2}r_i$ $(\forall i)$.

PROOF OF LEMMA. Without loss of generality, we may assume that

$$r_{i+1} > \tfrac{1}{2}r_i. \tag{1}$$

(Otherwise, $r_{i+2} < r_{i+1} \leq \frac{1}{2}r_i$ and we're done.) The Euclidean Algorithm gives $r_i = r_{i+1}q_{i+2} + r_{i+2}$, whereupon (1) forces $q_{i+2} = 1$.

[1]Actually, before the 1940s, "computer" meant "a person who performs computations"!

So

$$r_{i+2} = r_i - r_{i+1} \underset{(1)}{<} r_i - \tfrac{1}{2}r_i = \tfrac{1}{2}r_i.$$

□

PROOF OF THEOREM 17. The Lemma gives

$$(0 \leq)\ r_{2k} < \tfrac{1}{2}r_{2k-2} < \tfrac{1}{4}r_{2k-4} < \cdots < \tfrac{1}{2^{k-1}}r_2 < \tfrac{1}{2^k}b, \tag{2}$$

since b is essentially "r_0".

Suppose that $n > 2\log_2(b)$. Then $2^n > \left(2^{\log_2 b}\right)^2 = b^2$, and so $b < 2^{\frac{n}{2}}$. If n is even, then (2) yields $r_n < \frac{1}{2^{\frac{n}{2}}}b < 1 \implies r_n = 0$; if n is odd, then $r_{n+1} < \frac{1}{2^{\frac{n+1}{2}}}b < \frac{1}{\sqrt{2}} \implies r_{n+1} = 0$. In either case $r_{n+1} = 0$, which is what we had to show. □

EXAMPLE 19. Consider the pair $a = 85652$, $b = 16261$. We apply Theorem 16, constructing the table

			5	3	1	2	1	6
r	85652	16261	4357	3220	1127	966	161	0
x	1	0	1	-3	4	-11	15	–
y	0	1	-5	16	-21	58	-79	–

in which the top line denotes the values of q_i at each step. We conclude that

$$15a - 79b = 161 = (85652, 16261).$$

Note that $2\log_2 16261$ is close to 28, so we got somewhat lucky here.

Exercises

(1) Use induction to show that $8 \mid 5^{2n} + 7$.
(2) Show that no integers X and Y exist satisfying $(X, Y) = 3$ and $X + Y = 100$.
(3) Use the Euclidean algorithm to compute the GCD of $A = 7469$ and $B = 2464$.
(4) In problem (3), find x and y in $\mathbb{Z}$ such that $Ax + By = (A, B)$.

(5) Let $a, b \in \mathbb{N}$, and suppose that there are integers u and v satisfying $au + bv = 6$. Does the GCD (a, b) have to be 6? If not, what are its possible values?

CHAPTER 2

Primes and factorization

There are two ways to define the primes in $\mathbb{N}$. In the more general "rings of algebraic numbers" we'll meet later in the course, version (a) generalizes to define "irreducible elements" and version (b) to define "prime elements" (and these notions need not agree).

DEFINITION 20. A natural number $p > 1$ is prime if

[vers. (a)] for any $n \in \mathbb{N}$, $n|p \implies n = 1$ or $n = p$.
[vers. (b)] for any $a, b \in \mathbb{Z}$, $p|ab \implies p|a$ or $p|b$.

Wait! Are these equivalent? Let's check:

$\underline{(b) \implies (a)}$. If $n|p$, then $p = nm$, and so $p|nm$. By (b), $p|n$ or $p|m$. But then $p \leq n \leq nm = p$ (or $p \leq m \leq mn = p$) $\implies p = n$ (or m) $\implies n = p$ or 1. □

$\underline{(a) \implies (b)}$. Suppose $p|ab$ but $p \nmid b$; we wish to show that $p|a$. By (a), only 1 and p divide p, so $1 = (b, p) = bx + py$ (for some $x, y \in \mathbb{Z}$). Hence $a = abx + apy$, which is divisible by p since ab is. □

More generally we have the

PROPOSITION 21. *If $p|a_1 \cdots a_k$, then $p|a_i$ for some i.*

PROOF. Apply the above repeatedly: if $p \nmid a_1$, then $p|a_2 \cdots a_k$; if $p \nmid a_2$, then $p|a_3 \cdots a_k$; etc. □

Here is an application, to be generalized in the exercises.

THEOREM 22. *Let p be a prime. Then $\sqrt{p}$ is irrational.*

PROOF. Suppose $\sqrt{p} = \frac{A}{B}$, for $A, B \in \mathbb{N}$. Writing $a = \frac{A}{(A,B)}$, $b = \frac{B}{(A,B)}$, we have $\sqrt{p} = \frac{a}{b}$, $(a,b) = 1$. So

$$pb^2 = a^2 \implies p|a^2 \underset{\text{Prop.21}}{\implies} p|a \implies a = pc$$

and then $pb^2 = p^2c^2 \implies b^2 = pc^2 \implies p|b^2 \implies p|b$. But then $p|a, b$ in contradiction to $(a,b) = 1$. □

We turn to the main result of this section:

THEOREM 23 (Fundamental Theorem of Arithmetic). *Any natural number $n > 1$ has (up to reordering factors) a unique factorization*

$$n = p_1 p_2 \cdots p_s$$

into (not necessarily distinct) primes.

PROOF. To see the existence of a prime factorization, inductively assume that one exists for all $m < n$. Either n is prime (and we're done) or it is divisible by more than just 1 and n; in the latter case, say $n = mm'$ (with $m, m' < n$). Apply the inductive assumption.

Uniqueness is more involved. Suppose we have two prime factorizations

$$q_1 q_2 \cdots q_t = n = p_1 p_2 \cdots p_s,$$

with $t \geq s$. Then

$$p_1|q_1 \cdots q_t \underset{\text{Prop.21}}{\implies} p_1|q_i \text{ for some } i.$$

After reordering we may assume $i = 1$, so

$$p_1|q_1 \underset{q_1 \text{ prime}}{\implies} p_1 = q_1 \implies q_2 \cdots q_t = p_2 \cdots p_s.$$

Continue this process (reordering if necessary), obtaining $q_2 = p_2$, $q_3 = p_3$, …, $q_s = p_s$. If $t \neq s$ then we get $q_{s+1} \cdots q_t = 1$ which doesn't work; so $t = s$ too. □

Rather than repeating primes in a product, it's nicer to write

$$n = p_1^{a_1} \cdots p_s^{a_s} = \prod_i p_i^{a_i} = \prod_{p \text{ prime}} p^{\text{ord}_p(n)},$$

where the "order" of a prime p in n is defined by

$$\mathrm{ord}_p(n) := \begin{cases} a_i, & \text{if } p = \text{some } p_i \\ 0, & \text{otherwise.} \end{cases}$$

In terms of the prime factorization, we get formulas for the GCD and LCM of two numbers $a, b \in \mathbb{N}$: with $a = \prod p^{\mathrm{ord}_p(a)}$, $b = \prod p^{\mathrm{ord}_p(b)}$,

$$(a,b) = \prod p^{\min\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}, \qquad [a,b] = \prod p^{\max\{\mathrm{ord}_p(a),\mathrm{ord}_p(b)\}}.$$

This very quickly recovers $(a,b)[a,b] = ab$.

REMARK 24. Why do we make such a fuss about uniqueness? Precisely because it fails in other "rings of algebraic numbers"! Consider

$$\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

which is closed under addition and multiplication, and introduce the norm map

$$\begin{aligned} \mathcal{N} : \mathbb{Z}[\sqrt{-5}] \setminus \{0\} &\longrightarrow \mathbb{N} \\ a + b\sqrt{-5} &\longmapsto (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2. \end{aligned}$$

We have $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, which implies that elements with *prime norm* can only be divided by ($\pm$)themselves and ($\pm$)1, i.e. they are "irreducible". But in the equation

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}]$, we have norms

$$4 \cdot 9 = 36 = 6 \cdot 6.$$

What is preventing us from breaking

$$2\,,\ 3\,,\ 1 + \sqrt{-5}\,, \text{ and } 1 - \sqrt{-5} \tag{3}$$

down further into elements of norms 2 *and* 3 *that would (hopefully) coincide?*

The answer is this: that the insolubility of $a^2 + 5b^2 = 2$ or 3 means that

there are no elements of norm 2 or 3!!

So the four numbers (3) are "irreducible" and uniqueness of factorization into irreducible elements *fails*. The degree of failure in a "ring of algebraic numbers" is recorded by its *class number*, which will be explained toward the end of this course.

Here is a nice application of the Fundamental Theorem of Arithmetic (FTA):

THEOREM 25 (Euclid). *There are infinitely many primes.*

PROOF. Suppose $\{p_1, \ldots, p_n\} \subset \mathbb{N}$ was a complete list of all primes. Set $N := p_1 p_2 \cdots p_s + 1$. By the FTA, we must have $N = p_1^{a_1} \cdots p_s^{a_s}$. Pick some i for which $a_i \neq 0$. Then $p_i | N$, which (absurdly) implies $p_i | 1$. □

REMARK 26. If we look at the numbers N suggested by this proof, we get

$$2+1=3, \;\; 2\cdot 3+1=7, \;\; 2\cdot 3\cdot 5+1=31,$$
$$2\cdot 3\cdot 5\cdot 7+1=211, \;\; 2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311,$$

but

$$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031=59\cdot 509.$$

So they aren't all prime.

In fact, we can stretch Euclid's argument a little to obtain

PROPOSITION 27. *There are infinitely many primes of the form* $4n-1$.

PROOF. First observe that the product of two numbers of the form $4n+1$ (not $4n-1$) is once again of this form:

$$(4n+1)(4m+1) = 4(4nm+n+m)+1.$$

Now suppose that $\{p_1, \ldots p_k\}$ is a complete list of the primes of the form $4n-1$, and set

$$N := 4p_1 \cdots p_k - 1.$$

Note that this is odd.

By the FTA, $N = q_1 \cdots q_t$ can be written as a product of (odd) primes. They cannot all be of the form $4m+1$, since then N would

be. So some q_i, say q_1, is of the form $4m-1$ so is one of the $\{p_j\}$, say p_1. That is, $p_1|(4p_1\cdots p_k-1)$, a clear contradiction. □

The exercises cover another case, that of primes of the form $6n-1$. As we shall see, there is a very general theorem that these results reflect, so that the primes appear to "saturate" $\mathbb{N}$ in some sense. But the following result, which says that there exist arbitrarily large gaps in the primes, gives close to the opposite impression:

PROPOSITION 28. *Given any $k \in \mathbb{N}$, there exist k consecutive composite natural numbers.*

PROOF. Here is an example:

$$(k+1)!+2,\ (k+1)!+3,\ \ldots,\ (k+1)!+k,\ (k+1)!+k+1$$

are (respectively) divisible by 2, 3, ..., k, $k+1$, and thus composite. □

Exercises

(1) If x and y are odd, show that x^2+y^2 cannot be a perfect square.
(2) (a) If n is composite, explain why n must have a prime factor $p \leq \sqrt{n}$.
(b) Optional but fun: write the numbers from 2 to 200, then cross out all proper[1] multiples of 2, and continue with all proper multiples of 3, 5, 7, 11, 13($> \sqrt{200}$) to find all prime numbers less than 200.
(3) Let $N = p_1^{a_1}\cdots p_n^{a_n}$. Prove that N cannot have a rational square root unless all a_i are even (in which case it has a square root in $\mathbb{N}$).
(4) Show that there are infinitely many primes of the form $6n-1$.
(5) If 2^n+1 is an odd prime for some integer n, prove that n is a power of 2. [Hint: how do you factor $x^{2k+1}+1$? Now suppose n is divisible by an odd number.] The numbers of this form which

[1] i.e. not equal to 2

actually are prime are called Fermat primes; the only known ones are 3, 5, 17, 257, and 65537.

(6) If $2^n - 1$ is an odd prime for some integer n, prove that n is itself prime. The numbers of this form which actually are prime are called Mersenne primes; the largest currently known prime number is of this type: see
http://primes.utm.edu/notes/by_year.html

(7) Let $f(x)$ be a polynomial of degree > 1, with integer coefficients. Prove that we cannot have $f(n)$ prime for every $n \in \mathbb{N}$. [Hint: if $f(j) = p$ is prime, show that p divides $f(j + kp) - f(j)$ hence $f(j + kp)$ for every $k \in \mathbb{Z}$.]

CHAPTER 3

The distribution of primes

In the last section we showed — via a Euclid-inspired, *algebraic* argument — that there are infinitely many primes of the form $p = 4n-1$ (i.e. $4n+3$). In fact, this is true for primes of the form $4n+1$ as well, and the *ratio* of primes of these two forms less than N tends to 1 as $N \to \infty$. We say that the primes are distributed "asymptotically equally" between $\{4n+1 \mid n \in \mathbb{N}\}$ and $\{4n-1 \mid n \in \mathbb{N}\}$.

More generally, taking $\mathbb{P} \subset \mathbb{N}$ to denote the primes,

$$\mathbb{N}_{a,b} := \{a + nb \mid n \in \mathbb{Z}\} \cap \mathbb{N},$$

and

$$\mathbb{P}_{a,b} := \mathbb{N}_{a,b} \cap \mathbb{P},$$

there is the famous **theorem on primes in arithmetic progressions**:

THEOREM 29 (Dirichlet, 1837). *Given $a, b \in \mathbb{N}$ such that $(a,b) = 1$, the set $\mathbb{P}_{a,b}$ is infinite. Moreover, for each fixed b, the primes are distributed asymptotically equally between the $\{\mathbb{P}_{a,b}\}_{\substack{0<a<b \\ (a,b)=1}}$.*

In the early 20th century, people began to notice that the $\mathbb{N}_{a,b}$ contained consecutive sequences of primes, e.g.

$$\begin{aligned} &\mathbb{N}_{3,4} \supset \{3, 7, 11\} \text{ [length 3]} \\ &\mathbb{N}_{7,30} \supset \{7, 37, 67, 97, 127, 157\} \text{ [length 6] } (1909) \\ &\mathbb{N}_{199,210} \supset \{199, 409, \ldots\} \text{ [length 10] } (1910) \end{aligned} \tag{4}$$

A sequence of length 11 wasn't found until 1999; the longest known today has length 26 (and begins with a 16-digit number). In light of this, the *theoretical* result is impressive:

THEOREM 30 (Green and Tao, 2004). *Given any k, there exist a and b such that k consecutive elements of $\mathbb{N}_{a,b}$ are prime.*

One question which may bug you (for instance, in relation to the sequences (4)) is:

- How do you know if a number N is prime?

Naively, it's enough to check that no number $\leq \sqrt{N}$ divides N, but we will find better methods later. A second question is:

- How can one construct primes?

There is no nice answer here — no known function which produces distinct primes (and only primes).[1]

There are many other longstanding riddles regarding the primes: for example,

CONJECTURE 31 (Goldbach). *Any even number is the sum of two primes.*

This is known up to 18 digits but not proved in general. (A famous result of Vinogradov from the 1930s says that any sufficiently large odd number is the sum of 3 primes.) Alternatively, one might try to go further than Theorem 30 and ask whether, given any k and b (with b even), there exist infinitely many sequences

$$\{m + b, m + 2b, \ldots, m + kb\}$$

consisting entirely of primes. Taking $k = 2$ yields the venerable

CONJECTURE 32 (de Polignac, 1849). *Given any even $b \in \mathbb{N}$, there exist infinitely many pairs $p, q \in \mathbb{P}$ with $p - q = b$.*

The case $b = 2$ is known as the **twin prime conjecture**. A spectacular and unexpected recent advance is:

THEOREM 33 (Zhang, 2013). *Conjecture 32 holds for some $b < 70,000,000$.*

Recent work has brought this upper bound down to 246, but for the moment, the twin prime conjecture remains open.

[1] In the exercises, you will verify that no polynomial function can possibly do this.

Dirichlet's L-functions. We now turn to the idea behind the proof of Dirichlet's theorem (in the special case $b = 4$), starting with Euler's *analytic* approach to the infinitude of primes. What follows is far from being rigorous.

Let $s > 1$, and consider the "Euler product"

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{p \text{ prime}} \left(1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots\right)$$

where we have expanded each factor $(1-p^{-s})^{-1}$ as a geometric series on the right. If we formally expand the right-hand product, then by the Fundamental Theorem of Arithmetic, each $n^{-s} = (p_1^{a_1} \cdots p_k^{a_k})^{-s} = p_1^{-a_1 s} \cdots p_k^{-a_k s}$ occurs *exactly once*[2] in the result, yielding

$$= 1 + 2^{-s} + 3^{-s} + 4^{-s} + 5^{-s} + 6^{-s} + \cdots$$

$$= \sum_{n \geq 1} n^{-s} =: \zeta(s),$$

the **Riemann zeta function**.

REMARK 34. The series converges for $s > 1$ in $\mathbb{R}$, by the integral comparison test

$$\sum_{n \geq 2} \frac{1}{n^s} < \int_1^\infty \frac{dx}{x^s} = \left[\frac{x^{-s+1}}{-s+1}\right]_1^\infty = \frac{1}{s-1},$$

and more generally for $Re(s) > 1$ in the complex numbers $\mathbb{C}$. One may "analytically continue" it to get an analytic function on $\mathbb{C}\backslash\{1\}$ (with a simple pole at 1).

Now what could some analytic function have to do with the distribution of primes? Quite a bit: to begin with, formally taking the limit of the above as $s \to 1^+$ gives

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-1}} = \sum_{n \geq 1} \frac{1}{n} = \infty,$$

which "proves" the infinitude of primes.[3]

[2] because there *exists* a *unique* prime factorization of each $n \in \mathbb{N}$

[3] In mathematics, "formally" often means "manipulating symbols", which is about as far from rigor as one gets (and is great for producing or conveying ideas but also

The idea of Dirichlet's proof is to refine this observation. Let

$$\chi_0(n) := \begin{cases} 0, & n \text{ even} \\ 1, & n \text{ odd} \end{cases}$$

and

$$\chi_1(n) := \begin{cases} 0, & n \text{ even} \\ 1, & n = 4k+1 \\ -1, & n = 4k+3 \end{cases};$$

you should check that

$$\chi_i(mn) = \chi_i(m)\chi_i(n) \tag{5}$$

for $m, n \in \mathbb{N}$ (and $i = 0, 1$). We now carry out an analogue of the above argument, but in reverse, starting with the *Dirichlet series* (or *L-function*)

$$L(\chi_i, s) := \sum_{n \geq 1} \frac{\chi_i(n)}{n^s}$$

which using the Fundamental Theorem and (5) becomes

$$= \prod_{p \text{ prime}} \left(\sum_{k \geq 0} \frac{\chi_i(p^k)}{p^{ks}} \right) = \prod_{p \text{ prime}} \left(\sum_{k \geq 0} \left(\frac{\chi(p)}{p^s} \right)^k \right)$$

$$= \prod_{p \text{ prime}} \frac{1}{1 - \frac{\chi_i(p)}{p^s}}. \tag{6}$$

Taking log of (6) yields

$$\log L(\chi_i, s) = - \sum_{p \text{ prime}} \log \left(1 - \frac{\chi_i(p)}{p^s} \right),$$

which using $-\log(1-x) = \sum_{k \geq 1} \frac{x^k}{k}$ becomes

$$= \sum_{p \text{ prime}} \sum_{k \geq 1} \frac{\chi_i(p^k)}{k p^{ks}} = \sum_{p \text{ prime}} \frac{\chi_i(p)}{p^s} + \underbrace{\sum_{p \text{ prime}} \sum_{k \geq 2} \frac{\chi_i(p^k)}{k p^{ks}}}_{=: f_i(s)}.$$

---

can be terrifically misleading). For a proof without the quote marks, see the next subsection.

We can bound this last term (for $i = 0$ or 1) by

$$|f_i(s)| \leq \sum_{p \text{ prime}} \sum_{k \geq 2} \frac{1}{kp^{ks}} \leq \sum_{p \text{ prime}} \sum_{k \geq 2} \frac{1}{(p^s)^k} = \sum_{p \text{ prime}} \frac{p^{-2s}}{1 - p^{-s}}$$
$$\leq 2 \sum_{p \text{ prime}} p^{-2s} \leq 2 \sum_{n \geq 1} n^{-2s}$$

which for $s \geq 1$ is

$$\leq 2 \sum_{n \geq 1} \frac{1}{n^2} \leq 4.$$

Finally, using

$$\frac{\chi_0(n) + \chi_1(n)}{2} = \begin{cases} 1, & n = 4k+1 \\ 0, & \text{otherwise} \end{cases}$$

and

$$\frac{\chi_0(n) - \chi_1(n)}{2} = \begin{cases} 1, & n = 4k+3 \\ 0, & \text{otherwise} \end{cases},$$

we have

$$\frac{1}{2}\left(\log L(\chi_0, s) + \log L(\chi_1, s)\right) = \frac{f_0 + f_1}{2} + \underbrace{\sum_{\substack{p \text{ prime} \\ p = 4k+1}} \frac{1}{p^s}}_{\text{(A)}} \tag{7}$$

and

$$\frac{1}{2}\left(\log L(\chi_0, s) - \log L(\chi_1, s)\right) = \frac{f_0 - f_1}{2} + \underbrace{\sum_{\substack{p \text{ prime} \\ p = 4k+3}} \frac{1}{p^s}}_{\text{(B)}}. \tag{8}$$

Since $L(\chi_1, 1) = \sum \frac{\chi_1(n)}{n}$ converges by the alternating series test (with nonzero limit $\frac{\pi}{4}$), only the $\log L(\chi_0, s)$ and $\sum_p$ terms of (7) and (8) diverge as $s \to 1^+$. It follows that (A) and (B) diverge at the same rate. This proves that there are infinitely many primes of the form $4k + 1$, and suggests that they are distributed asymptotically equally to those of the form $4k + 3$.

The infinitude of primes. Finally, we shall describe one way of making Euler's argument above completely airtight, which has the added bonus of putting a lower bound on partial sums of inverse primes.

LEMMA 35. *$e^{x+x^2} \geq \frac{1}{1-x}$ for $x \in [0, \frac{1}{2}]$. (In particular, $e^{\frac{1}{p}+\frac{1}{p^2}} \geq \frac{1}{1-\frac{1}{p}}$ for each prime p.)*

PROOF. It suffices to show that

$$(1-x)e^{x+x^2} \geq 1.$$

The left-hand side of this is 1 at $x = 0$ and has derivative $x(1-2x)e^{x+x^2} \geq 0$ for $x \in [0, \frac{1}{2}]$. □

THEOREM 36. *For any real number $y > 2$,*

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p} > \log(\log y) - 1.$$

COROLLARY 37. *$\sum_{p \text{ prime}} \frac{1}{p}$ diverges. (In particular, there are infinitely many primes.)*

PROOF OF THEOREM 36. Given $y > 2$, set

$$\mathcal{N}_y := \left\{ n \in \mathbb{N} \;\middle|\; n = p_1^{a_1} \cdots p_k^{a_k}, \text{ all } p_i \leq y \right\},$$

and denote the greatest integer less than or equal to y by $\lfloor y \rfloor$. Now using the lemma together with the Fundamental Theorem, we find

$$\begin{aligned}
\prod_{\substack{p \le y \\ p \text{ prime}}} e^{\frac{1}{p}+\frac{1}{p^2}} &\ge \prod_{\substack{p \le y \\ p \text{ prime}}} \frac{1}{1-\frac{1}{p}} \\
&= \prod_{\substack{p \le y \\ p \text{ prime}}} \left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right) \\
&= \sum_{n \in \mathcal{N}_y} \frac{1}{n} \\
&\ge \sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} \underset{(\int \text{ test})}{\ge} \int_1^{1+\lfloor y \rfloor} \frac{dx}{x} = \log(1+\lfloor y \rfloor) \\
&> \log(y).
\end{aligned}$$

Taking log of both sides,

$$\begin{aligned}
\log\log y &< \log\left(\prod_{p \le y \text{ prime}} e^{\frac{1}{p}+\frac{1}{p^2}}\right) \\
&= \sum_{\substack{p \le y \\ p \text{ prime}}} \left(\frac{1}{p}+\frac{1}{p^2}\right) \\
&< \sum_{\substack{p \le y \\ p \text{ prime}}} \frac{1}{p} + \sum_{n=2}^{\infty} \frac{1}{n^2},
\end{aligned}$$

which by the integral test is

$$< \sum_{\substack{p \le y \\ p \text{ prime}}} \frac{1}{p} + \underbrace{\int_1^{\infty} \frac{dx}{x^2}}_{<1}.$$

□

In the next section, we will study the function

$$\pi(x) := \text{number of primes less than or equal to } x$$

on $\mathbb{R}_+ = (0, \infty)$. As a preliminary step, we can push Theorem 36 a bit further to get

COROLLARY 38. *For $x > 2$,*

$$\frac{\pi(x)}{x} + \int_2^x \frac{\pi(u)}{u^2} du > \log(\log x) - 1.$$

PROOF. Write $\pi(u) = \sum_{p \text{ prime}} \chi_{[p,\infty)}(u)$, where for any subset $\mathscr{S} \subset \mathbb{R}$,

$$\chi_{\mathscr{S}}(u) := \begin{cases} 1, & u \in \mathscr{S} \\ 0, & u \notin \mathscr{S} \end{cases}$$

is the characteristic function. Then we have[4]

$$\begin{aligned}
\int_2^x \frac{\pi(u)}{u^2} du &= \sum_{p \text{ prime}} \int_2^x \frac{\chi_{[p,\infty)}(u)}{u^2} du \\
&= \sum_{\substack{p \leq x \\ p \text{ prime}}} \int_p^x \frac{du}{u^2} \\
&= \sum_{\substack{p \leq x \\ p \text{ prime}}} \left[-\frac{1}{u} \right]_p^x \\
&= \sum_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{p} - \sum_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{x} \\
&= \sum_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{p} - \frac{\pi(x)}{x} \\
&\underset{\text{(Thm.)}}{>} \log(\log x) - 1 - \frac{\pi(x)}{x},
\end{aligned}$$

as desired. □

[4]Note that only finitely many terms of the sum contribute, so switching with the integral is permissible.

CHAPTER 4

The prime number theorem

So far, in our discussion of the distribution of the primes, we have not directly addressed the question of how their density in the natural numbers changes as one keeps counting. But we did at least define the function $\pi(x)$, which counts the number of primes $\leq x$, and you might wonder

- how fast does it grow?

or maybe

- is the answer good for anything?

Though we certainly shouldn't expect any fireworks from obseriving that

$$\frac{\pi(x)}{x} < 1,$$

we can at least put it together with the inequality

$$\frac{\pi(x)}{x} + \int_2^x \frac{\pi(u)}{u^2} du > \log(\log x) - 1$$

from Corollary I.C.10 to get that

$$F(x) := \int_2^x \frac{\pi(u)}{u^2} du - \log(\log x) + 2 > 0.$$

It follows that the derivative

$$F'(x) = \frac{\pi(x)}{x^2} - \frac{1}{x \log x}$$

must have nonnegative "lim sup".[1] Multiplying by $x \log x$, we find that

$$\limsup_{x \to \infty} \frac{\pi(x)}{x/\log x} - 1 \geq 0$$

[1] This means that given any negative constant, and any $M \gg 0$, there exists $x > M$ such that $F'(x)$ exceeds this constant. (Otherwise $F(x)$ would go negative.)

hence

$$\limsup_{x\to\infty} \frac{\pi(x)}{x/\log x} \geq 1,$$

which is to say that "there are a lot of primes". A better result is the **Prime Number Theorem**:

THEOREM 39 (de la Vallée Poussin/Hadamard, 1896). *We have*

$$\pi(x) \sim \frac{x}{\log(x)},$$

i.e. $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$ *exactly.*

This was already conjectured by Gauss and Legendre in the 1790s based on numerical evidence, perhaps of the sort in the following table:

x	10	100	1000	10^4	10^5	$\cdots$
$\pi(x)$	4	25	168	1229	9592	$\cdots$
$\frac{x}{\pi(x)}$	2.5	4.0	6.0	8.1	10.4	$\cdots$

Notice that the differences between the bottom entries stabilize to roughly $2.3 \sim \log 10$, which suggests

$$\frac{10^k}{\pi(10^k)} \sim k\log(10) = \log(10^k),$$

which then suggests (if you are Gauss or Legendre) Theorem 39.

IDEA OF THE PROOF. This uses complex analysis, and is based on the study of three functions:

$$\varphi(x) := \sum_{\substack{p \leq x \\ p \text{ prime}}} \log(p)\ ; \tag{9}$$

$$\Phi(s) := s\int_1^\infty \frac{\varphi(x)}{x^{s+1}}dx\ ; \tag{10}$$

and the Riemann zeta function

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \underbrace{\prod_{p \text{ prime}} \frac{1}{1-p^{-s}}}_{\text{Euler product}}. \tag{11}$$

What can (11) possibly have to do with (9) and (10)?

We start by expressing (10) as a series: $\Phi(s) =$

$$s \sum_{p \text{ prime}} \int_p^\infty \frac{(\log p)dx}{x^{s+1}} = s \sum_p \left[\frac{-\log p}{sx^s} \right]_p^\infty = \sum_{p \text{ prime}} \frac{\log p}{p^s},$$

which apparently makes sense (like (11)) for complex numbers s with $Re(s) > 1$. Now use $-\frac{d}{ds} p^{-s} = (\log p) p^{-s}$ to write

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{d}{ds} \log \zeta(s) = \frac{d}{ds} \sum_{p \text{ prime}} \left(-\log(1 - p^{-s}) \right) = \sum_{p \text{ prime}} \frac{\log p}{p^s(1 - p^{-s})},$$

and notice that by expanding $\frac{1}{1-p^{-s}}$ this becomes $\Phi(s) + H(s)$ where H (which involves $\frac{1}{p^{2s}}$+higher) is analytic for $Re(s) > \frac{1}{2}$. The reason why this is important, is that

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n \geq 1} \frac{1}{n^s} - \int_1^\infty \frac{1}{x^s} dx \\ &= \sum_{n \geq 1} \int_n^{n+1} \underbrace{\left(\frac{1}{n^s} - \frac{1}{x^s} \right)}_{\leq \frac{|s|}{n^{Re(s)+1}}} dx \end{aligned}$$

extends to an analytic function on $Re(s) > 0$. Moreover, the Euler product converges on $Re(s) > 1$, from which we see that $\zeta(s)$ has no zeroes there, and a deeper analysis shows that $\zeta(s)$ has no zeroes on (or accumulating to) $Re(s) = 1$ — just the *pole* at $s = 1$.

The upshot of this discussion is that $\Phi(s)$ *extends to an analytic function on* $Re(s) > \frac{1}{2}$, *except for poles at* $s = 1$ *and poles at zeroes of* $\zeta(s)$ *(with* $Re(s) < 1 - \epsilon$*).* In particular, we conclude from this that the function

$$g(s) = \int_1^\infty \frac{\varphi(x) - x}{x^{s+1}} dx = \frac{\Phi(s)}{s} - \frac{1}{s-1}$$

is analytic in a neighborhood of $s = 1$. The integral only converges *a priori* for $Re(s) > 1$, but a deep "Tauberian theorem" in complex analysis shows that since (among other things) g extends through 1,

the integral actually does converge there: i.e., we have

$$\int_1^\infty \frac{\varphi(x) - x}{x^2} dx < \infty,$$

which implies $\frac{\varphi(x)-x}{x} \to 0$ as $x \to \infty$, hence

$$\lim_{x\to\infty} \frac{\varphi(x)}{x} = 1. \tag{12}$$

To finish off the Prime Number Theorem, write

$$\varphi(x) = \sum_{\substack{p \le x \\ p \text{ prime}}} \log(p) \le \sum_{\substack{p \le x \\ p \text{ prime}}} \log(x) = \pi(x)\log(x) \tag{13}$$

and (for $1 < y < x$)

$$\pi(x) = \pi(y) + \sum_{\substack{p \in (y,x] \\ p \text{ prime}}} \le \pi(y) + \sum_{p \in (y,x]} \frac{\log p}{\log x} < y + \frac{\varphi(x)}{\log y}. \tag{14}$$

Taking $y = \frac{x}{\log^2 x}$, multiplying (14) by $\frac{\log x}{x}$ and (13) by $\frac{1}{x}$, gives

$$\begin{aligned}\frac{\varphi(x)}{x} < \pi(x)\frac{\log x}{x} &< \left(\frac{x}{\log^2 x} + \frac{\varphi(x)}{\log x - 2\log\log x}\right)\frac{\log x}{x} \\ &= \frac{1}{\log x} + \frac{\varphi(x)}{x}\frac{\log x}{\log x - 2\log\log x}.\end{aligned}$$

By (12), the end terms of this inequality limit to 1 as $x \to \infty$; therefore $\pi(x)\frac{\log x}{x} \to 1$ also — so that the beast is, in the end, tamed by the "squeeze theorem" from Calculus. □

In fact we know more about $\zeta(s)$: it extends to an analytic function on all of $\mathbb{C}$ (except for the pole at 1), with zeroes:

- at negative even integers; and
- in the "critical strip" $0 < Re(s) < 1$ — these are called the "critical zeroes".

For an easy $1,000,000, you should prove

CONJECTURE 40 (The Riemann Hypothesis). *The critical zeroes are all on* $Re(s) = \frac{1}{2}$.

The PNT was proved using some of what we know about $\zeta(s)$. One might expect that an even better result would follow from Conjecture 40. In fact, the function

$$Li(x) := \int_0^x \frac{dt}{\log t}$$

is known to do a better job than $\frac{x}{\log(x)}$ at approximating $\pi(x)$, and the better result would use this instead:

THEOREM 41 (Schoenfield, 1976). *If the Riemann Hypothesis holds, then*

$$|\pi(x) - Li(x)| \leq \frac{1}{8\pi}\sqrt{x}\log(x)$$

for all $x \geq 2657$.

There are many other consequences: to mention just one more, recall that Proposition I.B.9 says that there exist gaps of arbitrary length between the primes. On the other hand, one may have to look at very large numbers just to get a small gap. If the RH holds, then (according to a result of Cramér) we can make this last statement very precise: the gap between prime p and the next prime is bounded by a constant times $\sqrt{p}\log(p)$.

An application of the Prime Number Theorem. Here's the "what is it good for" part: we'll use the PNT to prove that

$$\zeta(3) = \sum_{n\geq 1} \frac{1}{n^3}$$

is irrational. Set $d_n := \text{lcm}\{1, 2, 3, \ldots, n\}$(=product of prime powers$\leq n$).

LEMMA 42. $d_n < 3^n$ *for n sufficiently large.*

PROOF. To begin with,

$$d_n = \prod_{\substack{p \le n \\ p \text{ prime}}} p^{\lfloor \log_p n \rfloor} < \prod_{\substack{p \le n \\ p \text{ prime}}} p^{\log_p n} = n^{\pi(n)}.$$

Now let $\epsilon > 0$ be such that $e^{1+\epsilon} < 3$. By the PNT, there exists $N \in \mathbb{N}$ such that

$$\begin{aligned} n \ge N &\implies \pi(n) < (1+\epsilon)\frac{n}{\log n} \\ &\implies \pi(n)\log n < (1+\epsilon)n \\ &\underset{\exp}{\implies} n^{\pi(n)} < e^{(1+\epsilon)n} = (e^{1+\epsilon})^n < 3^n. \end{aligned}$$

□

LEMMA 43. *For $s > r \in \mathbb{N}$,*

(a) $$\int_0^1 \int_0^1 \frac{-\log xy}{1-xy} x^r y^r dx\, dy = 2\zeta(3) - \underbrace{\left(1 + \frac{1}{2^3} + \cdots + \frac{1}{r^3}\right)}_{\in \frac{1}{d_r^3}\mathbb{Z}}$$

(b) $$\int_0^1 \int_0^1 \frac{-\log xy}{1-xy} x^r y^s dx\, dy \in \frac{1}{d_s^3}\mathbb{Z}.$$

PROOF OF (A) ((B) IS SIMILAR). Write

$$\int_0^1 \int_0^1 \frac{x^{t+r}y^{t+r}}{1-xy} dx\, dy = \sum_{k\ge 0} \int_0^1 \int_0^1 x^{t+r+k} y^{t+r+k} dx\, dy = \sum_{k \ge 0} \frac{1}{(t+r+k+1)^2}.$$

Differentiate with respect to t (using $\frac{d}{dt}x^t = x^t \log x$), set $t = 0$

$$\implies \int_0^1 \int_0^1 \frac{\log xy}{1-xy} dx\, dy = -2 \sum_{k \ge 0} \frac{1}{(r+k+1)^3}.$$

□

Now define the *Legendre polynomials*

$$P_n(x) := \frac{1}{n!}\left(\frac{d}{dx}\right)^n x^n (1-x)^n.$$

LEMMA 44. *For $n \in \mathbb{N}$,*

$$\int_0^1 \int_0^1 \frac{-\log xy}{1-xy} P_n(x)P_n(y)dx\,dy \leq (\sqrt{2}-1)^{4n} 2\zeta(3).$$

SKETCH. Notice that $P_n(x)P_n(y)$ is a sum of terms of the form $x^r y^s$. By Lemma 43, the integral equals $\frac{1}{d_n^3}(A_n + \zeta(3)B_n)$ for some $A_n, B_n \in \mathbb{Z}$. The rest is complicated integration by parts and bounding. □

THEOREM 45 (Apéry, 1978). $\zeta(3) \notin \mathbb{Q}$.

PROOF. Since the integral in Lemma 44 is nonzero, we have for each $n \in \mathbb{N}$

$$0 < \frac{|A_n + \zeta(3)B_n|}{d_n^3} < 2\zeta(3)(\sqrt{2}-1)^{4n}.$$

Therefore

$$\begin{aligned} 0 < |A_n + \zeta(3)B_n| < \quad & 2\zeta(3)d_n^3(\sqrt{2}-1)^{4n} \\ \underset{\text{Lemma 42}}{<} \quad & 2\zeta(3)(\underbrace{3^3(\sqrt{2}-1)^4}_{<0.9})^n \\ < \quad & 2\zeta(3)(0.9)^n. \end{aligned}$$

Suppose $\zeta(3) = \frac{P}{Q}$, for some nonzero $P, Q \in \mathbb{Z}$. Then the above yields

$$0 < |A + \tfrac{P}{Q}B_n| < 2\tfrac{P}{Q}(0.9)^n$$

hence for n large enough

$$0 < |A_nQ + PB_n| < 2P(0.9)^n < 1,$$

which is impossible since $A_nQ + PB_n$ is an integer. □

That $3^3(\sqrt{2}-1)^4$ is less than 1 is a miracle. Many similar would-be proofs (e.g., for Catalan's constant) fail solely because the corresponding number exceeds 1!

So the irrationality of $\zeta(3)$ is a really deep fact, which uses the Prime Number Theorem among other things. Not all irrationality proofs are hard – for instance, the one for $\sqrt{2}$ is very easy. The first 2 problems below will walk you through a somewhat more interesting

(but still straightforward) method that works for e, $\sin(1)$, and other numbers. They don't involve the PNT.

Exercises

(1) Let θ be a real number and a_m and b_m two sequences of integers (with the b_m's nonzero). Suppose that for every $\epsilon > 0$, there exists an $M \in \mathbb{N}$ such that

$$m \geq M \implies 0 < \left| \theta - \frac{a_m}{b_m} \right| < \frac{\epsilon}{b_m}.$$

Show that θ is irrational.

(2) Suppose that $f(x)$ is a function represented by a power series (say, about 0 for simplicity) on the whole real line, and write $f(x) = P_k(x) + R_k(x)$ as a sum of the k^{th} Taylor polynomial and remainder. Recall from calculus that

$$R_k(x) = \int_0^x \frac{f^{(k+1)}(t)}{k!}(x-t)^k dt.$$

Apply this formula with $f(x) := e^x$, and problem (1), to show that e is irrational.

(3) Explain why the PNT would lead you to expect that, on average, the gap between the prime p and its successor is $\log(p)$.

Part 2

Congruences

CHAPTER 5

Modular arithmetic

Leaving our brief dip into the analytic aspects of number theory behind us, we turn to the algebraic approach which will inform our discussion of cryptography. I assume no prior acquaintance with ring or group theory, but as this is not a course in abstract algebra, we will be selective in what we do cover.

Let m, a, and b be three integers, with $m \geq 2$.

DEFINITION 46. a is **congruent to** b **modulo** $m \iff m|(a-b)$. (Equivalently, a and b have the same remainder when divided by m in the Euclidean Algorithm.) The notation for this is "$a \underset{(m)}{\equiv} b$" or "$a \equiv b \pmod{m}$".

REMARK 47. We can also say "b is a residue of a modulo m".

Now "$\underset{(m)}{\equiv}$" is an **equivalence relation** on $\mathbb{Z}$: it satisfies

- reflexivity : $a \underset{(m)}{\equiv} a$;
- symmetry : $a \underset{(m)}{\equiv} b \implies b \underset{(m)}{\equiv} a$; and
- transitivity : $a \underset{(m)}{\equiv} b$ and $b \underset{(m)}{\equiv} c \implies a \underset{(m)}{\equiv} c$.

Accordingly, $\mathbb{Z}$ is partitioned into **equivalence classes**. Explicitly, these are the m arithmetic progressions

$$m\mathbb{Z},\ 1+m\mathbb{Z},\ 2+m\mathbb{Z},\ \ldots,\ (m-1)+m\mathbb{Z}.$$

They are called **residue** (or **congruence**) **classes modulo** m. A **complete set of residues modulo** m is a set of m integers with no two in the same residue class; e.g., for $m = 3$, $\{0,1,2\}$ will work, as will $\{0,2,4\}$.

Next, "$\underset{(m)}{\equiv}$" respects addition, subtraction, and multiplication: if $a \underset{(m)}{\equiv} b$ and $c \underset{(m)}{\equiv} d$, then:

- $a + c \underset{(m)}{\equiv} b + d$;
- $-c \underset{(m)}{\equiv} -d$ ($\implies a - c \underset{(m)}{\equiv} b - d$); and
- $ac \underset{(m)}{\equiv} bd$.

Repeatedly using these shows also that

- $f(a) \underset{(m)}{\equiv} f(b)$ for any polynomial f with integer coefficients.

The upshot is that we may work with only $0, 1, 2, \ldots, m-1$ — i.e., with a complete set of residues — when doing arithmetic modulo m. The set of residue classes, endowed with "$+$" and "$\cdot$", is written $\mathbb{Z}/m\mathbb{Z}$ and called **the ring of integers modulo** m.

REMARK 48. People often write $a + m\mathbb{Z}$, $\bar{a}$, or $[a]$ for the element of $\mathbb{Z}/m\mathbb{Z}$ corresponding to $a \in \mathbb{Z}$.

EXAMPLE 49. Let $n \in \mathbb{N}$, and write $n = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^ka_k$. We have

$$10 \underset{(9)}{\equiv} 1 \implies 10^j \underset{(9)}{\equiv} 1 \implies n \underset{(9)}{\equiv} a_0 + a_1 + \cdots + a_k,$$

so that $9|n \iff$ 9 divides the sum of the digits of n. On the other hand,

$$10 \underset{(11)}{\equiv} -1 \implies 10^j \underset{(11)}{\equiv} (-1)^j \implies n \underset{(11)}{\equiv} a_0 - a_1 + \cdots + (-1)^k a_k$$

reveals that $11|n \iff$ 11 divides the *alternating* sum of the digits of n.

EXAMPLE 50 (Fast powering algorithm). To compute $5^5 \pmod{11}$, we need not actually compute 5^5 and then apply the Euclidean Algorithm. Rather, apply EA at each step:

$$\begin{aligned}
5^2 &= 25 \underset{(11)}{\equiv} 3 \\
5^3 = 5^2 \cdot 5 &\underset{(11)}{\equiv} 3 \cdot 5 = 15 \underset{(11)}{\equiv} 4 \\
5^4 = 5^3 \cdot 5 &\underset{(11)}{\equiv} 4 \cdot 5 = 20 \underset{(11)}{\equiv} 9 \\
5^5 = 5^4 \cdot 5 &\underset{(11)}{\equiv} 9 \cdot 5 = 45 \underset{(11)}{\equiv} 1.
\end{aligned}$$

But if we want (say) 5^{13}, this is wasteful. Instead, compute

$$5^2 \underset{(11)}{\equiv} 3, \;\; 5^4 = (5^2)^2 \underset{(11)}{\equiv} 3^2 = 9, \;\; 5^8 = (5^4)^2 \underset{(11)}{\equiv} 9^2 = 81 \underset{(11)}{\equiv} 4$$

$$\implies 5^{13} = 5^{8+4+1} \underset{(11)}{\equiv} 4 \cdot 9 \cdot 5 = 180 \underset{(11)}{\equiv} 4.$$

(In fact, using Fermat's theorem below will give an even faster shortcut.) The general algorithm here for finding $a^e \pmod{m}$ is to write the exponent in binary, compute all the a^{2^i} you need, then multiply them together. This reduces us from computing e multiplications to $\leq 2 \log_2 e$ multiplications mod m.[1]

What about division, and inverses?

DEFINITION 51. Given $a \in \mathbb{Z}$, an **inverse of** a **modulo** m is an integer $b \in \mathbb{Z}$ such that $a \cdot b \underset{(m)}{\equiv} 1$. (If one exists, a is **invertible mod** m, and we shall write "a^{-1}" for b.)

THEOREM 52. *(i) a is invertible mod $m \iff (a, m) = 1$.*

(ii) In this case, the "inverses of a" are the elements of a single congruence class.

[1] In the exercises you will see how to virtually eliminate the storage aspect of this algorithm.

PROOF. If $a \cdot b \underset{(m)}{\equiv} 1$, then $ab - 1 = cm$ (for some $c \in \mathbb{Z}$) hence $(a, m)|ab - cm = 1$. Conversely, if $x, y \in \mathbb{Z}$ are such that $ax + my = 1$, then $ax \underset{(m)}{\equiv} 1$. This proves (i).

For (ii), given $ab \underset{(m)}{\equiv} 1 \underset{(m)}{\equiv} ab'$, we have $0 \underset{(m)}{\equiv} a(b - b')$, which multiplied by any inverse a^{-1} yields $0 \underset{(m)}{\equiv} b - b'$ hence $b \underset{(m)}{\equiv} b'$. □

In fact, the proof of (i) shows us how to find inverses: use the EA to find x and y.

EXAMPLE 53. Can we invert 48 (mod 157)? The EA allows us to simultaneously check whether these numbers are relatively prime, and if so, to perform the computation:

			3	3	1	2	4
r	157	48	13	9	4	1	0
x	1	0	1	-3	4	-11	–
y	0	1	-3	10	-13	36	–

We conclude that $-11 \cdot 157 + 36 \cdot 48 = 1$, hence $36 \cdot 48 \underset{(157)}{\equiv} 1$, which is to say $48^{-1} \underset{(157)}{\equiv} 36$.

REMARK 54. Of course, the inverse is really an inverse in $\mathbb{Z}/m\mathbb{Z}$, and it is better to write $[48]^{-1} = [36]$ in the example. Theorem 52(ii) says that the inverse of an invertible element of $\mathbb{Z}/m\mathbb{Z}$ is a *unique* element of $\mathbb{Z}/m\mathbb{Z}$.

COROLLARY 55. *$ax \underset{(m)}{\equiv} ay$ and $(a, m) = 1 \implies x \underset{(m)}{\equiv} y$.*

PROOF. Multiply both sides by any mod-m-inverse of a. □

COROLLARY 56. *If $\{x_1, \ldots, x_m\}$ is a complete set of residues mod m, and $(a, m) = 1$, then so is $\{ax_1, \ldots, ax_m\}$.*

PROOF. By Corollary 55, multiplication by a gives a 1-to-1 mapping from $\mathbb{Z}/m\mathbb{Z}$ to itself. □

How many of the residue classes are invertible? Denote these by $(\mathbb{Z}/m\mathbb{Z})^* \subset \mathbb{Z}/m\mathbb{Z}$.

DEFINITION 57. (a) [Euler's phi-function][2] $\phi(m) := |(\mathbb{Z}/m\mathbb{Z})^*| = \#\{a \in \{0, 1, \ldots, m-1\} \mid (m, a) = 1\}$.

(b) A **reduced residue system (mod m)** is a set of $\phi(m)$ integers relatively prime to m, with no two in the same mod-m-residue class (e.g. $\{a \in \{0, 1, \ldots, m-1\} \mid (m, a) = 1\}$).

REMARK 58. The equality of the two definitions of $\phi(m)$ is by Theorem 52.

EXAMPLE 59. A couple of values of the phi-function:

$$\phi(15) = \#\{1, 2, 4, 7, 8, 11, 13, 14\} = 8,$$

$$\phi(11) = \#\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = 10.$$

Now remember from Example 50 that $5^5 \underset{(11)}{\equiv} 1$. So $5^{10} \underset{(11)}{\equiv} 1$. Try

$$2^{10} = 2^{2+8} = 4 \cdot 4^4 \underset{(11)}{\equiv} 4 \cdot 5^2 \underset{(11)}{\equiv} 4 \cdot 3 \underset{(11)}{\equiv} 1$$

$$3^{10} = 9 \cdot 9^4 \underset{(11)}{\equiv} -2 \cdot (-2)^4 \underset{(11)}{\equiv} -2 \cdot 5 \underset{(11)}{\equiv} -10 \underset{(11)}{\equiv} 1$$

and so on — we always get 1. Except, of course, for $0^{10}(= 0)$. On the other hand, for the modulus 15, we have

$$2^8 \underset{(15)}{\equiv} 4^4 \underset{(15)}{\equiv} 1^2 = 1, \quad 7^8 \underset{(15)}{\equiv} 4^4 \underset{(15)}{\equiv} 1, \text{ etc.}$$

but

$$3^8 = 9^4 \underset{(15)}{\equiv} 6^2 \underset{(15)}{\equiv} 6 \underset{(15)}{\not\equiv} 1 \text{ !!}$$

The following theorem sums up and generalizes the behavior we have just witnessed:

THEOREM 60 (Euler). $(a, m) = 1 \implies a^{\phi(m)} \underset{(m)}{\equiv} 1$.

PROOF. Consider the reduced residue system

$$R_m := \{r \in \{1, \ldots, m-1\} \mid (r, m) = 1\}.$$

[2]Recall that the number of elements in a set S is denoted by $|S|$ or $\#S$.

Since $(a,m) = 1 = (r,m) \implies (ar,m) = 1$, and multiplication by a is 1-to-1 on $\mathbb{Z}/m\mathbb{Z}$, aR_m is also a reduced residue system. Hence

$$\prod_{r\in R_m} r \underset{(m)}{\equiv} \prod_{s\in aR_m} s = \prod_{r\in R_m} ar = a^{\phi(m)} \prod_{r\in R_m} r.$$

Cancelling the r's (by Corollary 55), we have $1 = a^{\phi(m)}$. □

COROLLARY 61 (Fermat's "Little" Theorem). *Let a be an integer, and p a prime not dividing a. Then $a^{p-1} \underset{(p)}{\equiv} 1$.*

PROOF. $\phi(p) = p - 1$. Apply Theorem 60. □

EXAMPLE 62. What weekday will we have $1,000,000$ days from today? (Today is Monday.) By Fermat, $10^6 \underset{(7)}{\equiv} 1 \implies$ Tuesday!

Exercises

(1) Evaluate $\phi(m)$ for $m = 1, 2, 3, \ldots, 12$.
(2) Prove that $n^{13} - n$ is divisible by $2, 3, 5, 7$, and 13 for any integer n.
(3) Let m be an odd integer and let a be any integer. Prove that $2m + a^2$ can never be a perfect square. [Hint: if a number is a square, what are its possible values modulo 4?]
(4) Let N, g, and A be positive integers. Consider the following algorithm:
   1. Set $a = g$ and $b = 1$.
   2. Loop while $A > 0$.
      3. If $A \equiv 1$ (mod 2), set $b = b \cdot a$ (mod N).
      4. Set $a = a^2$ (mod N) ad $A = \lfloor \frac{A}{2} \rfloor$.
      5. If $A > 0$, continue with loop at Step 2.
   6. Return the number b.
   (a) Show that the output of this algorithm equals g^A (mod N).
   (b) Use it to compute 17^{183} (mod 256).
(5) For each of the following primes p and numbers a, compute a^{-1} mod p in two ways: (i) using the Euclidean algorithm; (ii) use problem (7) and Fermat's little theorem.

(a) $p = 47$ and $a = 11$.
(b) $p = 587$ and $a = 345$.

CHAPTER 6

Consequences of Fermat's theorem

Orders of residue classes. Recall that by Fermat's Little Theorem, $p \nmid a \implies a^{p-1} \underset{(p)}{\equiv} 1$. But perhaps there are smaller powers of a that are $\underset{(p)}{\equiv} 1$?

DEFINITION 63. Let $a, m \in \mathbb{Z}$, with $m \geq 2$ and $(a, m) = 1$. The **order** of a modulo m is the smallest $k \in \mathbb{N}$ such that $a^k \underset{(m)}{\equiv} 1$.

PROPOSITION 64. *Assume $(a, m) = 1$ as in the definition. Then the order of a mod m divides $\phi(m)$. (In particular, for p prime and $p \nmid a$, the order of a mod p divides $p - 1$.)*

PROOF. Let k be the order and $a^n \underset{(m)}{\equiv} 1$. Writing $n = kq + r$, $0 \leq r \leq k$, we have $1 \underset{(m)}{\equiv} (a^k)^q a^r \underset{(m)}{\equiv} a^r$, contradicting minimality of k unless $r = 0$ (so that k divides n). Now use Euler's Theorem 60 (and take $n = \phi(m)$). □

The question arises whether there is any a with order *exactly* $\phi(m)$. For prime modulus ($m = p$), such an *a does* exist, and then its powers $a^1, \ldots, a^{p-1}$ give (together with 0) a complete set of residue classes (mod p). (We'll see why later.) Otherwise, this may fail: for instance, $\phi(8) = 4$ but $1^2, 3^2, 5^2, 7^2 \underset{(8)}{\equiv} 1 \implies$ the residue classes (other than 0 and 1) all have order 2.

Solutions of congruences. We are interested in solving congruences of the form

$$f(x) \underset{(m)}{\equiv} 0, \tag{15}$$

where $f(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients. (Usually one takes $m \nmid a_n$.) Since $a \underset{(m)}{\equiv} b \implies f(a) \underset{(m)}{\equiv} f(b)$, all the elements of a given residue class $a + m\mathbb{Z}$ either solve (15) or don't. It therefore makes sense to think of the set of solutions as a subset of $\mathbb{Z}/m\mathbb{Z}$; in particular, there are (in this sense) finitely many.

EXAMPLE 65. Let p be prime. By Fermat, $x^{p-1} - 1 \underset{(p)}{\equiv} 0$ has $p-1$ solutions (in $\mathbb{Z}/p\mathbb{Z}$), and so $x^p - x \underset{(p)}{\equiv} 0$ has p solutions (in $\mathbb{Z}/p\mathbb{Z}$). This is something that doesn't happen with equations "over $\mathbb{Z}$": the only polynomial that has $f(a) = 0$ for every $a \in \mathbb{Z}$ is *zero*!

We shall now discuss some linear and quadratic congruences, starting with the linear case. Recall that

$$ca \underset{(m)}{\equiv} cb \implies a \underset{(m)}{\equiv} b \quad \text{if } (c, m) = 1.$$

There is a more general statement:

LEMMA 66. $ca \underset{(m)}{\equiv} cb \iff a \underset{\left(\frac{m}{(c,m)}\right)}{\equiv} b.$

PROOF. First assume $m | c(a-b)$. Then $\frac{m}{(m,c)} | \frac{c}{(m,c)}(a-b)$, but $\frac{m}{(m,c)}$ and $\frac{c}{(m,c)}$ are relatively prime. Invoking Corollary 13(ii), we have $\frac{m}{(m,c)} | a - b$.

For the converse, assume $a \underset{(\frac{m}{(c,m)})}{\equiv} b$; then certainly $ca \underset{(\frac{cm}{(c,m)})}{\equiv} cb$, and $\frac{cm}{(c,m)} = [c, m]$ (the lcm). Since $m | [c, m]$, $ca \underset{(m)}{\equiv} cb$. □

THEOREM 67. *(i) $ax - b \underset{(m)}{\equiv} 0$ has a solution if and only if $(a, m) | b$.*

(ii) In this case, there are (in $\mathbb{Z}/m\mathbb{Z}$) exactly (a, m) solutions.

PROOF. (i) Write $g := (a, m)$. The existence of a solution is equivalent to the existence of $x, y \in \mathbb{Z}$ such that $ax + my = b$. This clearly implies $g | b$ since $g | a, m$. Conversely, if $b = g\beta$ then write $a = g\alpha$, $m = g\mu$; since $(\alpha, \mu) = 1$, α has an inverse $\tilde{\alpha}$ mod μ. (Here $\tilde{\alpha} \in \mathbb{Z}$.) Take $x_0 := \tilde{\alpha}\beta$ so that $\alpha x_0 \underset{(\mu)}{\equiv} \beta$, and thus $g\alpha x_0 \underset{(g\mu)}{\equiv} g\beta$, i.e. $ax_0 \underset{(m)}{\equiv} b$.

(ii) By the Lemma, $ax \underset{(m)}{\equiv} b$ is equivalent to $\alpha x \underset{(\mu)}{\equiv} \beta$. So the *distinct* solutions in $\mathbb{Z}/m\mathbb{Z}$ are $\tilde{\alpha}\beta, \tilde{\alpha}\beta + \mu, \ldots, \tilde{\alpha}\beta + (g-1)\mu$. □

EXAMPLE 68. We solve $15x \underset{(35)}{\equiv} 25$. This is equivalent to $3x \underset{(7)}{\equiv} 5$, and the mod 7 inverse of 3 is 5. So $x_0 \underset{(7)}{\equiv} 5 \cdot 5 \underset{(7)}{\equiv} 4$ is one solution; and the complete list is $4, 11, 18, 25, 32$ (add 7 each time).

Let $p \geq 2$ be a prime.

Going back to Fermat's theorem, it makes intuitive sense that if we think in terms of polynomials *with* $\mathbb{Z}/p\mathbb{Z}$*-coefficients*, $f(x)$ should have a linear factor $(x - r)$ for every r with $f(r) \underset{(p)}{\equiv} 0$. I won't prove this now; instead consider what it *suggests*: namely, that $x^{p-1} - 1$ should factor as the product $(x-1)(x-2)\cdots(x-(p-1))$, since $1, 2, \ldots, p-1$ are all roots. This would imply

$$(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1) \underset{(p)}{\equiv} -1,$$

since there is an even number of factors. This is part of what shall be proved in the next subsection.

The quadratic congruences $x^2 \underset{(p)}{\equiv} 1$ and $x^2 \underset{(p)}{\equiv} -1$.

LEMMA 69. $x^2 \underset{(p)}{\equiv} 1 \iff x \underset{(p)}{\equiv} \pm 1$.

PROOF. Well, $x^2 - 1 \underset{(p)}{\equiv} 0$ is equivalent to $p|(x+1)(x-1)$, right? Which is the same as $p|(x-1)$ or $p|(x+1)$. □

THEOREM 70 (Wilson's Theorem). *For any prime* p, $(p-1)! \underset{(p)}{\equiv} -1$.

PROOF. Obvious for $p = 2, 3$. For $p \geq 5$, write

$$-(p-1)! = (1-p) \cdot \prod_{j=2}^{p-2} j$$

$$\underset{(p)}{\equiv} \prod_{j=2}^{p-2} j. \tag{16}$$

In $\{2, \ldots, p-2\}$, nothing is its *own* mod p inverse, by the Lemma. So in the product (16), everything pairs off with its onverse to yield $1 \pmod{p}$. □

Turning to $x^2 \underset{(p)}{\equiv} -1$, we note that for $p = 2$ we have $-1 \underset{(2)}{\equiv} 1$, so this has $x \equiv \pm 1$ as solutions. So assume $p > 2$.

COROLLARY 71. $x^2 \underset{(p)}{\equiv} -1$ *is soluble* $\iff p \underset{(4)}{\equiv} 1$.

PROOF. By Theorem 70, we have

$$-1 \underset{(p)}{\equiv} \prod_{j=1}^{\frac{p-1}{2}} j(p-j) = \prod_{j=1}^{\frac{p-1}{2}} (-j^2),$$

which implies

$$(-1)^{\frac{p+1}{2}} \underset{(p)}{\equiv} \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2.$$

If $p = 4n+1$, then $(-1)^{\frac{p+1}{2}} = (-1)^{2n+1} = -1$ and we can take $x = \prod_{j=1}^{\frac{p-1}{2}} j$.

Conversely, suppose $x_0^2 \underset{(p)}{\equiv} -1$. Fermat's theorem tells us that $1 \underset{(p)}{\equiv} x_0^{p-1} = (x_0^2)^{\frac{p-1}{2}} \underset{(p)}{\equiv} (-1)^{\frac{p-1}{2}}$, and so $\frac{p-1}{2}$ must be even, which means that $p \underset{(4)}{\equiv} 1$. □

In algebraic number theory, one of the first things one studies is the factorization of integer primes in certain[1] quadratic number rings of the form

$$\mathcal{O}_{\sqrt{d}} := \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z}, & d \underset{(4)}{\not\equiv} 1 \\ \mathbb{Z} + \frac{\sqrt{d}+1}{2}\mathbb{Z}, & d \underset{(4)}{\equiv} 1 \end{cases}$$

[1] It only works precisely this way when "$\mathcal{O}_{\sqrt{d}}$ has class number 1".

where $d \in \mathbb{Z}$. One finds that for $p > 2$ prime,

$$p \begin{cases} = \alpha\bar{\alpha} & \text{if } d \underset{(p)}{\equiv} \square \underset{(p)}{\not\equiv} 0 \\ = \alpha^2 & \text{if } p|d \\ \text{doesn't factor} & \text{if } d \underset{(p)}{\not\equiv} \square \end{cases}$$

where "$\square$" means "a square" (i.e. x^2 for some integer x), and if $\alpha = A + B\sqrt{d}$ then $\bar{\alpha} = A - B\sqrt{d}$. This is an amazing symmetry: the factorization behavior of d mod p — basically whether $x^2 - d \underset{(p)}{\equiv} 0$ is soluble — determines the factorization behavior of p in the "extension" $\mathcal{O}_{\sqrt{d}}$ of $\mathbb{Z}$!

We shall use Corollary 71 to prove this in the special case $d = -1$: again, let $p > 2$ be prime.

THEOREM 72. *There exist $a, b \in \mathbb{N}$ such that $p = a^2 + b^2$ if and only if $p \underset{(4)}{\equiv} 1$.*

Notice that the first statement is really that $p = (a+bi)(a-bi) = \alpha\bar{\alpha}$, while the second is equivalent to $(d =) -1 \underset{(p)}{\equiv} \square$ by the Corollary.

PROOF. If $p \underset{(4)}{\equiv} 1$, then (by Corollary 71) there is an $x \in \mathbb{Z}$ with $x^2 \underset{(p)}{\equiv} -1$. Set $f(u,v) := u + xv$, $\mathcal{S} := \{(u,v) \mid u, v \in \mathbb{Z} \cap [0, \sqrt{p}]\}$. Since $|\mathcal{S}| = (\lfloor\sqrt{p}\rfloor + 1)^2 > p$, the elements $\{f(u,v) \bmod p \mid (u,v) \in \mathcal{S}\}$ in $\mathbb{Z}/p\mathbb{Z}$ cannot all be distinct. So there exist (in $\mathcal{S}$) $(u,v) \neq (u',v')$ with $f(u,v) \underset{(p)}{\equiv} f(u',v')$. Writing $a := u - u'$, $b := v - v'$, this gives $a \underset{(p)}{\equiv} xb$, hence (squaring both sides) $a^2 \underset{(p)}{\equiv} -1 \cdot b^2$, which is to say $a^2 + b^2 \underset{(p)}{\equiv} 0$, i.e. $p|a^2 + b^2$. As $u, u', v, v' \in [0, \sqrt{p}]$, we have $a, b < \sqrt{p}$ (and not both 0) $\implies 0 < a^2 + b^2 < 2p$. But since $p|a^2 + b^2$, we must then have $p = a^2 + b^2$.

On the other hand, if $p = a^2 + b^2$, then one of a, b must be odd (say, $a = 2n+1$) and the other even (say, $b = 2m$). So $p = (2n+1)^2 + (2m)^2 = 4(n^2 + n + m^2) + 1$. $\square$

REMARK 73. We can actually prove something stronger:

$$\text{if } p|a^2+b^2 \text{ and } p \underset{(4)}{\equiv} 3, \text{ then } p|a,b.$$

Otherwise a is invertible mod p, and writing $aa' \underset{(p)}{\equiv} 1$, $a^2+b^2 \underset{(p)}{\equiv} 0$ multiplied by $(a')^2$ yields $1+(a'b)^2 \underset{(p)}{\equiv} 0$; by Corollary 71 we then have $p \underset{(4)}{\equiv} 1$.

COROLLARY 74. *Let n be a natural number. The following are equivalent:*

(a) $n = a^2+b^2$ for some $a, b \in \mathbb{Z}$;

(b) in the prime factorization of n, the primes of the form $4m+3$ occur to even powers.

PROOF. Note that (a) says that $n = \alpha\bar{\alpha}$, $\alpha \in \mathbb{Z}+i\mathbb{Z}$. Clearly a product of numbers of this form is also of this form. By Theorem 72, any prime of the form $4m+1$ is of this form. Also, the square of any integer (in particular, of a prime of the form $4m+3$) is also of this form. So if (b) holds, then (a) holds.

Now assume (a). The Remark above shows that if a prime p of the form $4m+3$ divides a^2+b^2, so does its square, and also $p|a,b$. Replace n, a, b by $\frac{n}{p^2}$, $\frac{a}{p}$, $\frac{b}{p}$ and continue in this fashion. If (b) does not hold then we evidently must reach a contradiction. □

This connects up to an earlier discussion, in §I.B: the numbers a^2+b^2 ($a, b \in \mathbb{Z}$) are exactly the norms of the Gaussian integers.

Exercises

(1) Let p be a prime. Show that exactly half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are squares (modulo p).

(2) If p is an odd prime, prove that $1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \underset{(p)}{\equiv} (-1)^{\frac{p+1}{2}}$ and $2^2 \cdot 4^2 \cdot 6^2 \cdot \cdots \cdot (p-1)^2 \underset{(p)}{\equiv} (-1)^{\frac{p+1}{2}}$.

(3) How many solutions are there to $15x \underset{(35)}{\equiv} 0$? $15x \underset{(35)}{\equiv} 24$?

(4) Find all solutions to $x^2 \underset{(2^\alpha)}{\equiv} 1$ for each $\alpha = 1, 2, 3, \ldots$. (For $\alpha \geq 3$, $2^{\alpha-1} - 1$ and $2^{\alpha-1} + 1$ should be among your solutions. Start by factoring $x^2 - 1$ and thinking about what the linear factors have to be to have product zero modulo 2^α.)

CHAPTER 7

The Chinese Remainder Theorem

We have been concerned with solving the equation

$$f(x) \underset{(m)}{\equiv} 0\,, \quad f \text{ polynomial}, \tag{17}$$

primarily (so far) when the modulus m is prime. What if m is composite? Can we reduce the problem of solving (17) to the case of a prime power modulus?

Here is a related problem, from Sun Tzu around 300 AD:

EXAMPLE 75. We wish to find $x \in \mathbb{Z}$ simultaneously solving

$$\begin{cases} x \underset{(3)}{\equiv} 2 & \text{(i)} \\ x \underset{(5)}{\equiv} 3 & \text{(ii)} \\ x \underset{(7)}{\equiv} 2 & \text{(iii)}. \end{cases}$$

First observe that (i) $\implies x = 2 + 3y$ ($y \in \mathbb{Z}$). Combining this with (ii) gives

$$2 + 3y \underset{(5)}{\equiv} 3,$$

or $3y \underset{(5)}{\equiv} 1$. Since the mod 5 inverse of 3 is 2, we have $y \underset{(5)}{\equiv} 2$ hence $y = 2 + 5z$ ($z \in \mathbb{Z}$). Finally, by (iii),

$$2 \underset{(7)}{\equiv} x = 2 + 3y = 2 + 3(2 + 5z) = 8 + 15z \underset{(7)}{\equiv} 1 + z$$

whence $z \underset{(7)}{\equiv} 1$ and $z = 1 + 7w$ ($w \in \mathbb{Z}$). Therefore (for any integer w)

$$x = 2 + 3(2 + 5(1 + 7w)) = 23 + 105w$$

will work. Notice that $105 = 3 \cdot 5 \cdot 7$.

THEOREM 76 (Chinese Remainder Theorem). *Given $m, n > 1$ coprime, and $a, b \in \mathbb{Z}$, there exists an integer x satisfying*

$$x \underset{(m)}{\equiv} a\,, \quad x \underset{(n)}{\equiv} b\,, \tag{18}$$

which is unique if we demand $0 \leq x < mn$.

PROOF. We have (18) $\iff x = a + my \underset{(n)}{\equiv} b \iff my \underset{(n)}{\equiv} b - a$. Since $(m, n) = 1$, m is invertible mod n; let[1] $\beta \in \mathbb{Z}$ satisfy $\beta m \underset{(n)}{\equiv} 1$. Then (18) $\iff y \underset{(n)}{\equiv} \beta(b-a) \iff y = \beta(b-a) + nz \iff$

$$x = a + m\beta(b-a) + mnz.$$

Exactly one choice of z puts $x \in [0, mn)$. □

EXAMPLE 77. Consider the congruences

$$\begin{cases} x \underset{(52)}{\equiv} 29 \\ x \underset{(72)}{\equiv} 19. \end{cases}$$

We have $(52, 72) = 4$, so the basic CRT (Theorem 76) doesn't apply. Still, we can try the method: write $x = 29 + 52y \underset{(72)}{\equiv} 19 \implies 52y \underset{(72)}{\equiv} -10$. By Theorem II.B.5, this is solvable if and only if $(52, 72)$ divides -10, which fails (as $(52, 72) = 4$). So a common solution to these congruences does not exist.[2]

Here are two generalizations of Theorem 76:

THEOREM 78 (CRT v. 2.0). *Given $m, n > 1$ and $a, b \in \mathbb{Z}$. Then there exists an integer x satisfying* (18) *if and only if $a \underset{(m,n)}{\equiv} b$. In this case, there is a unique solution $0 \leq x < [m, n]$.*

PROOF. See the exercises. □

[1] You would find β using the Euclidean Algorithm.

[2] A quicker way to see this: $x \underset{(52)}{\equiv} 29 \implies x \underset{(4)}{\equiv} 29 \underset{(4)}{\equiv} 1$, since $4|52$; and $x \underset{(72)}{\equiv} 19 \implies x \underset{(4)}{\equiv} 19 \underset{(4)}{\equiv} 3$, since $4|72$. This is a contradiction.

THEOREM 79 (CRT v. 3.0). *Let $m_1, \dots, m_r > 1$ be pairwise coprime, and $a_1, \dots, a_r \in \mathbb{Z}$. Then there exists an integer solving the system $\{x \underset{(m_i)}{\equiv} a_i\}_{i=1,\dots,r}$, which is unique if we impose $0 \leq x < m := \prod_{i=1}^r m_i$.*

PROOF. We could, as in Example 75, iterate the approach used in proving the basic CRT. A more systematic approach is this: for each i, $(\frac{m}{m_i}, m_i) = 1 \implies \exists \alpha_i \in \mathbb{Z}$ such that $\alpha_i \cdot \frac{m}{m_i} \underset{(m_i)}{\equiv} 1$. Moreover, $\frac{m}{m_j} \cdot \alpha_i \underset{(m_i)}{\equiv} 0$ if $j \neq i$, since $m_i | \frac{m}{m_j}$. Setting

$$x_0 := \sum_{j=1}^r \frac{m}{m_j} \alpha_j a_j,$$

we have (for each i)

$$x_0 \underset{(m_i)}{\equiv} \underbrace{\frac{m}{m_i} \alpha_i}_{\equiv 1} a_i \underset{(m_i)}{\equiv} a_i.$$

If x, x' are two solutions, $x - x' \underset{(m_i)}{\equiv} 0 \ (\forall i) \implies m_i | x - x' \ (\forall i) \underset{\text{coprime}}{\overset{m_i}{\implies}}$ $m | x - x' \implies x' = x + mz$, which gives the uniqueness statement. □

Now let $(m, n) = 1$ and consider the map

$$\begin{array}{rccccc} \Theta: & \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} & \times & \mathbb{Z}/n\mathbb{Z} \\ & [x]_{mn} & \longmapsto & ([x]_m & , & [x]_n). \end{array}$$

The content of the basic CRT is that

Θ is 1-to-1 and onto (i.e. a bijection):

the existence statement says that any $([a]_m, [b]_n)$ is $\Theta([x]_{mn})$ for some $x \in \mathbb{Z}$; while the uniqueness says that all such x lie in a *single* residue class $[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$. (In terms of counting, this is plausible, since $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ both have mn elements.)

REMARK 80. Dropping the assumption that $(m,n)=1$ for a moment, Theorem 78 says that in

$$\begin{array}{ccccc} \mathbb{Z}/[m,n]\mathbb{Z} & \xrightarrow{\Theta} & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} & \xrightarrow{\Psi} & \mathbb{Z}/(m,n)\mathbb{Z} \\ [x]_{[m,n]} & \longmapsto & ([x]_m,[x]_n) & & \\ & & ([a]_m,[b]_n) & \longmapsto & [a-b]_{(m,n)} \end{array}$$

the image of Θ is exactly the kernel of Ψ (stuff Ψ sends to zero).

Henceforth we take (m,n) to be 1.

If we consider *invertible* elements, we get that Θ restricts to a bijection[3]

$$(\mathbb{Z}/mn\mathbb{Z})^* \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^*\times(\mathbb{Z}/n\mathbb{Z})^*, \tag{19}$$

since $(x,mn)=1 \iff \{(x,m)=1 \text{ and } (x,n)=1\}$. But then the two sides of (19) must have the same number of elements. It follows that the Euler phi-function is "multiplicative":

THEOREM 81. *If $(m,n)=1$, then $\phi(mn)=\phi(m)\phi(n)$.*

If $N=\prod_i p_i^{r_i}$ (where p_i denote *distinct* primes), this result leads to the formula

$$\phi(N)=\prod_i \phi(p_i^{r_i})=\prod_i p^{r_i}\left(1-\tfrac{1}{p_i}\right)$$

since

$$\begin{aligned} \phi(p^r) &= \#\{a\in\{1,\dots,p^r\}\,|\,p\nmid a\} \\ &= \#\left(\{1,2,\dots,p^r\}\setminus\{p,2p,\dots,p^{r-1}p\}\right) \\ &= p^r-p^{r-1}=p^r\left(1-\tfrac{1}{p}\right). \end{aligned}$$

Finally (still assuming $(m,n)=1$), if we consider elements solving a polynomial congruence

$$(\mathbb{Z}/N\mathbb{Z})_f := \left\{[x]\in\mathbb{Z}/N\mathbb{Z}\,\middle|\, f(x)\underset{(N)}{\equiv}0\right\},$$

[3]We will use the symbol "$\cong$" to denote bijections.

then Θ restricts to a bijection

$$(\mathbb{Z}/mn\mathbb{Z})_f \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})_f \times (\mathbb{Z}/n\mathbb{Z})_f$$

since $f(x) \underset{(mn)}{\equiv} 0 \iff mn|f(x) \underset{(m,n)=1}{\iff} \{m|f(x) \text{ and } n|f(x)\} \iff \{f(x) \underset{(m)}{\equiv} 0 \text{ and } f(x) \underset{(n)}{\equiv} 0\}$. Writing

$$\mathcal{N}_f(N) := \left|(\mathbb{Z}/N\mathbb{Z})_f\right| = \#\text{ of solutions mod } N,$$

we have

THEOREM 82. *If $(m,n) = 1$, then $\mathcal{N}_f(mn) = \mathcal{N}_f(m)\mathcal{N}_f(n)$; i.e. $\mathcal{N}_f$ is multiplcative in the same sense as ϕ.*

EXAMPLE 83. We can use Theorem 82 to determine the square roots of 34 modulo 55 — that is, to solve $f(x) \underset{(55)}{\equiv} 0$ where $f(x) = x^2 - 34$.

First, we solve mod 5: $x^2 \underset{(5)}{\equiv} 34 \equiv 4 \implies x \underset{(5)}{\equiv} 2, -2 \equiv 2, 3$; then solve mod 11: $x^2 \underset{(11)}{\equiv} 34 \equiv 1 \implies x \underset{(11)}{\equiv} \pm 1$. The content of the argument leading to Theorem 82 is that we now just solve

$$\begin{cases} x \underset{(5)}{\equiv} 2, 3 \\ x \underset{(11)}{\equiv} \pm 1 \end{cases}$$

mod 55:

Case 1 : $x = 1 + 11a \underset{(5)}{\equiv} 2 \text{ or } 3 \implies a \underset{(5)}{\equiv} 1 \text{ or } 2 \implies x \underset{(55)}{\equiv} 12 \text{ or } 23.$

Case 2 : $x = -1 + 11a \underset{(5)}{\equiv} 2 \text{ or } 3 \implies a \underset{(5)}{\equiv} 3 \text{ or } 4 \implies x \underset{(55)}{\equiv} 32 \text{ or } 43.$

So, in $\mathbb{Z}/55\mathbb{Z}$, the number 34 has *four* square roots (!):

$$12,\ 23,\ 32,\ \text{and } 43.$$

Exercises

(1) Prove Theorem 78 (v. 2.0 of the Chinese Remainder Theorem).
(2) Find all integers that give the remainders $1, 2, 3$ when divided by $3, 4, 5$, respectively.
(3) For what values of n is $\phi(n)$ odd?

(4) Find all solutions to the congruence $x^3 + 4x + 8 \underset{(15)}{\equiv} 0$.

CHAPTER 8

Primality and compositeness testing

For cryptographic purposes (among others), it is important to be able to identify when a modulus is prime. More precisely, given $m \in \mathbb{N}$, we would like an algorithmic approach to the decision problems

(I) Is m prime?

(II) (a) Is m composite?

(b) If so, what is its prime factorization?

There are several "tests" that pop right out of the results of the last 3 chapters:

(1) Wilson: p prime $\implies (p-1)! \underset{(p)}{\equiv} -1$.

In fact, the converse holds too for p at least 5. Unfortunately, taking factorials to determine primeness (or compositeness) is usually slower than checking all the numbers $n \in \mathbb{Z} \cap [2, \sqrt{p}]$ for a divisor!

(2) Quadratic congruences: p prime $\implies x \underset{(p)}{\equiv} \pm 1$ are the only solutions to $x^2 \underset{(p)}{\equiv} 1$.

So, suppose you can produce $x \in \mathbb{Z}/m\mathbb{Z}$ not $\underset{(m)}{\equiv} \pm 1$ with $x^2 \underset{(m)}{\equiv} 1$: then m is *composite*. It turns out that such an x may be furnished by the *failure* of the next method to show compositeness (see Example 90).

(3) Little Fermat: p prime $\implies a^{p-1} \underset{(p)}{\equiv} 1$ for every $a \in \mathbb{Z} \cap [1, p-1]$.

That is, if you can find some $a \in \mathbb{Z} \cap [1, m-1]$ such that $a^{m-1} \underset{(m)}{\not\equiv} 1$, then m is *composite*. But what about showing something is prime?

(4) Converse Fermat: Given a natural number $m > 1$ such that $a^{m-1} \underset{(m)}{\equiv} 1$ for *every* $a \in \mathbb{Z} \cap [1, m-1]$. Then m is prime.

PROOF. Suppose instead that $m = n_1 n_2$, $n_i > 1$. By hypothesis, $a^{m-1} \underset{(m)}{\equiv} 1$ ($\forall a = 1, \ldots, m-1$), and so $a^{m-1} \underset{(n_1)}{\equiv} 1$ ($\forall a = 1, \ldots, m-1$) — in particular, $n_1^{m-1} \underset{(n_1)}{\equiv} 1$. But this is absurd, as $n_1 \underset{(n_1)}{\equiv} 0$. □

In other words, if m is composite then $a^{m-1} \underset{(m)}{\equiv} 1$ at least must fail for some *proper factor* a of m (i.e. $a|m$, $a \neq 1, m$).

In implementing **(3)-(4)**, we use the version of the fast-powering algorithm worked out in the exercises:

Algorithm: Given $N, g, A \in \mathbb{N}$,

1. Set $a := g$, $b := 1$.
2. If $A = 0$, go to Step 6.
3. If $A \underset{(2)}{\equiv} 1$, set $b :\underset{(N)}{\equiv} b \cdot a$.
4. Set $a :\underset{(N)}{\equiv} a^2$, $A := \lfloor \frac{A}{2} \rfloor$.
5. Go to Step 2.
6. Output b.

PROPOSITION 84. *The output is* $g^A \pmod N$.

PROOF. is by induction on A. The "base case" $A = 0$ is just that $g^0 = 1$.

The inductive step depends on whether A is odd or even. First assume $A \underset{(2)}{\equiv} 0$. Running the algorithm is equivalent to: replacing g by g^2, A by $\frac{A}{2}$, and running the algorithm. By the inductive assumption, the output (modulo N) is $(g^2)^{\frac{A}{2}} = g^A$.

If $A \underset{(2)}{\equiv} 1$, then running the algorithm is equivalent to: replacing g by g^2, A by $\frac{A-1}{2}$, running the algorithm, and multiplying the output[1] by g. The output, using the inductive assumption, is $g \cdot (g^2)^{\frac{A-1}{2}} = g \cdot g^{A-1} = g^A \pmod N$. □

[1]The initial multiplication in Step 3 may be moved to the end.

EXAMPLE 85. Is $m = 731$ prime or composite?
We compute 2^{m-1}, setting $a = 2$, $A = 730$, $N = 731$, $b = 1$.

- $A \underset{(2)}{\equiv} 0 \longrightarrow a := a^2 = 4$, $A := \frac{A}{2} = 365$.
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 4$, $a := a^2 = 16$, $A := \frac{A-1}{2} = 182$.
- $A \underset{(2)}{\equiv} 0 \longrightarrow a := a^2 = 256$, $A := \frac{A}{2} = 91$.
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 4 \cdot 256 = 1024 \underset{(m)}{\equiv} 293$, $a := a^2 = 65536 \underset{(m)}{\equiv} 65536 - \lfloor \frac{65536}{731} \rfloor 731 = 65536 - 89 \cdot 731 = 477$, $A = \frac{A-1}{2} = 45$. (The computation of a demonstrates how to use the division algorithm with the aid of a computer.)
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 293 \cdot 477 = 139761 \underset{(m)}{\equiv} 140$, $a := a^2 = 227529 \underset{(m)}{\equiv} 188$, $A := \frac{A-1}{2} = 22$.
- $A \underset{(2)}{\equiv} 0 \longrightarrow a := a^2 = 35344 \underset{(m)}{\equiv} 256$, $A := \frac{A}{2} = 11$.
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 140 \cdot 256 = 35840 \underset{(m)}{\equiv} 21$, $a := a^2 \underset{(m)}{\equiv} 477$, $A := \frac{A-1}{2} = 5$.
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 21 \cdot 477 = 10017 \underset{(m)}{\equiv} 514$, $a := a^2 = 188$, $A := \frac{A-1}{2} = 2$.
- $A \underset{(2)}{\equiv} 0 \longrightarrow a := a^2 \equiv 256$, $A := \frac{A}{2} = 1$.
- $A \underset{(2)}{\equiv} 1 \longrightarrow b := b \cdot a = 514 \cdot 256 = 131584 \underset{(m)}{\equiv} 4$, $a := a^2 \underset{(m)}{\equiv} 477$, $A := \frac{A-1}{2} = 0$.
- Output $b = 4 (\underset{(m)}{\equiv} 2^{730}) \underset{(m)}{\not\equiv} 1 \implies m$ composite.

REMARK 86. In fact, 731 has prime factorization $43 \cdot 17$, so $\phi(731) = \phi(43)\phi(17) = 42 \cdot 16 = 2^5 \cdot 3 \cdot 7$. As we saw in Proposition II.B.2, and shall see again in our discussion of groups, the order of any element of $(\mathbb{Z}/731\mathbb{Z})^*$ must divide $\phi(731)$, and we saw that $256^8 \underset{(m)}{\equiv} 256$; so 256 has order 7 (mod 731), which is consistent with this.

But this method is *not* always good at detecting composites. There are composite numbers m for which $a^{m-1} \underset{(m)}{\equiv} 1$ is *only* false for the proper factors $a|m$. Another way of saying this is the following:

(3′) Little Fermat v. 2: p prime $\implies a^p \underset{(p)}{\equiv} a$ $(\forall a \in \mathbb{Z})$.

DEFINITION 87. A **Carmichael number** is a natural number $m > 1$ for which "the converse of **(3')** fails": i.e. $a^m \underset{(m)}{\equiv} a$ $(\forall a \in \mathbb{Z})$ *and* m is composite.[2]

These are rare (about 2000 of them in the interval that contains the first 1 billion primes), but there are infinitely many, and we will want a method that doesn't essentially fail for some set of composite numbers.

THEOREM 88 (Korselt, 1899). *Let* $m = \prod p_i^{r_i}$ *be composite.* (*Here the* $\{p_i\}$ *are distinct primes dividing* m.) *Then*

$$m \text{ is Carmichael} \iff \text{all } r_i = 1 \text{ and } (p_i - 1)|(m-1).$$

PROOF OF $\Longleftarrow$ ($\Longrightarrow$ IS AN EXERCISE): Let $a \in \mathbb{Z}$. By Little Fermat (v. 2),

$$\begin{aligned}
a^{p_i} \underset{(p_i)}{\equiv} a \ (\forall i) \quad &\Longrightarrow \begin{cases} a^{p_i-1} \underset{(p_i)}{\equiv} 0 & \text{if } p_i|a \\ a^{p_i-1} \underset{(p_i)}{\equiv} 1 & \text{if } p_i \nmid a \end{cases} \quad (\forall i) \\
&\underset{(p_i-1)|(m-1)}{\overset{\text{all}}{\Longrightarrow}} \begin{cases} a^{m-1} \underset{(p_i)}{\equiv} 0 & \text{if } p_i|a \\ a^{m-1} \underset{(p_i)}{\equiv} 1 & \text{if } p_i \nmid a \end{cases} \quad (\forall i) \\
&\Longrightarrow \quad a^m \underset{(p_i)}{\equiv} a \ (\forall i) \\
&\Longrightarrow \quad p_i|(a^m - a) \ (\forall i) \\
&\underset{\text{all } r_i=1}{\Longrightarrow} \quad m = \operatorname{lcm}(\{p_i\})|(a^m - a),
\end{aligned}$$

which is to say $a^m \underset{(m)}{\equiv} a$. □

Note that all Carmichael numbers are odd, since at least one p_i must be odd, and then $p_i - 1$ (which divides $m - 1$) is even.

[2]Their existence might seem to contradict **(4)**; but this is not so, as $a^m \underset{(m)}{\equiv} a$ need not imply $a^{m-1} \underset{(m)}{\equiv} 1$ if $(a, m) \neq 1$.

EXAMPLE 89. The smallest Carmichael number is $m = 561 = 3 \cdot 11 \cdot 17$. (To apply Korselt's theorem, just note that $2 = 3 - 1$, $10 = 11 - 1$, and $16 = 17 - 1$ all divide 560.)

Traditionally an $a \in \mathbb{Z}$ for which $a^m \not\underset{(m)}{\equiv} a$ is called a **Fermat witness** for (the compositeness of) m; obviously Carmichael numbers are precisely the composites with no Fermat witnesses. One also says that if $a^{m-1} \underset{(m)}{\equiv} 1$, m is a "probable prime (to the base a)", and if m is also composite it is **pseudoprime** (to the base a). The worst case scenario, of being pseudoprime to every base coprime to m, is that of Carmichael numbers.

To see how compositeness criterion **(2)** enters, consider the following example of a non-Carmichael pseudoprime.

EXAMPLE 90. Is $m = 1387$ prime or composite?

As in Example 85, we try computing 2^{1386}, which mod 1387 gives 1. So m is a probable prime to the base 2. Set $x = 2^{693}$, so that $x^2 = 2^{1386} \underset{(m)}{\equiv} 1$. If $x \not\underset{(m)}{\equiv} \pm 1$, then m is composite; and indeed, one finds that x is 512.

This approach actually leads us to a test (namely, **(5)** below) that misses nothing — no Carmichael-like phenomena. It is based on

THEOREM 91. *Let $p > 2$ be prime, with $p - 1 = 2^k q$, q odd. Given $a \in (\mathbb{Z}/p\mathbb{Z})^*$, we have:*

(i) $a^q \underset{(p)}{\equiv} 1$; or

(ii) one of $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is $\underset{(p)}{\equiv} -1$.

PROOF. Let $a^{2^\alpha q}$ be the first number in the sequence

$$a^q,\ a^{2q},\ a^{4q},\ \ldots,\ a^{2^k q}$$

which is $\underset{(p)}{\equiv} 1$. If $\alpha = 0$, then $a^q \underset{(p)}{\equiv} 1$ and (i) holds.

If $\alpha \geq 1$, set $x := a^{2^{\alpha-1}q}$; then $x^2 \underset{(p)}{\equiv} 1$. By **(2)**, $x \underset{(p)}{\equiv} -1$. □

Let $m > 2$ be odd, and write $m - 1 = 2^k q$ (q odd). As an immediate consequence of Theorem 91, we have:

(5) Miller-Rabin: If $\exists a \in \mathbb{Z}$ coprime to m with $a^q \underset{(m)}{\not\equiv} 1$ and $a^{2^i q} \underset{(m)}{\not\equiv} -1$ ($i = 0, 1, \ldots, k-1$), then m is composite.

Such an "a" is a **Miller-Rabin witness** for (the compositeness of) m. If a is not a Miller-Rabin witness for m, then m is a "strong probable prime (to the base a)", and if m is also composite then it is a **strong pseudoprime** (to the base a).[3]

EXAMPLE 92. Again let $m = 561$. Then $m - 1 = 560 = 2^4 \cdot 35$. Use **(5)** to prove that m is composite (left to you).

The converse of **(5)** holds as promised, but in fact we have something even better:

THEOREM 93. *If m is composite, then at least $\frac{3}{4}$ of the elements $a \in \mathbb{Z} \cap [1, n-1]$ are Miller-Rabin witnesses for (or not coprime to) m.*

So: if the first ten a's you try don't provide a Miller-Rabin witness, m has a *very high probability* of being prime. It is *conjectured* that m is definitely prime if there are no witnesses in $\mathbb{Z} \cap [1, 2\log^2 m]$.

PROOF IN THE CASE[4] $m = p_1 \cdot \cdots \cdot p_r$, $r \geq 3$: By the Chinese Remainder Theorem,

$$(\mathbb{Z}/m\mathbb{Z})^* \underset{\Theta}{\overset{\cong}{\leftarrow}} (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^*;$$

note that Θ is compatible with taking powers.

[3] written "$spsp(a)$"

Write $p_j - 1 = 2^{k_j} q_j$ (q_j odd), and let $\ell := \min\{k, k_1, \ldots, k_r\}$. The set of *non*-(Miller-Rabin-)witnesses is[5]

$$L := \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^* \;\middle|\; \begin{array}{c} a^{2^k q} \underset{(m)}{\equiv} 1; \text{ and for } i = 0, 1, \ldots, k-1, \\ a^{2^{i+1} q} \underset{(m)}{\equiv} 1 \implies a^{2^i q} \underset{(m)}{\equiv} \pm 1 \end{array} \right\}.$$

Let $a \in L$. If ℓ' denotes the smallest power for which $a^{2^{\ell'} q} \underset{(m)}{\equiv} 1$ (we know $\ell' \leq k$), then $a^{2^{\ell'-1} q} \underset{(m)}{\equiv} -1$. This gives $a^{2^{\ell'-1} q} \underset{(p_j)}{\equiv} -1$ $(\forall j) \implies$ $a^{2^{\ell'} q} \underset{(p_j)}{\equiv} 1$ $(\forall j) \implies$ $2^{\ell'}$ divides the "mod p_j order" of a, which by Proposition II.B.2 divides $\phi(p_j) = 2^{k_j} q_j$. Therefore we must have $\ell' \leq k_j$ for each j, and so $\ell' \leq \ell$, hence (by definition of ℓ') $a^{2^\ell q} \underset{(m)}{\equiv} 1$.

Next, we have the inclusions of sets

$$\begin{aligned} L \subseteq H &:= \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^* \;\middle|\; a^{2^{\ell-1} q} \underset{(m)}{\equiv} \pm 1 \right\} \\ &\subseteq G := \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^* \;\middle|\; a^{2^\ell q} \underset{(m)}{\equiv} 1 \right\} \\ &\subseteq (\mathbb{Z}/m\mathbb{Z})^* \\ &\subseteq \{1, \ldots, m-1\}, \end{aligned}$$

[5]The set of Miller-Rabin witnesses in $(\mathbb{Z}/m\mathbb{Z})^*$ is

$$M := \left\{ a \in (\mathbb{Z}/m\mathbb{Z})^* \;\middle|\; \begin{array}{c} a^q \underset{(m)}{\not\equiv} 1; \text{ and for } i = 0, 1, \ldots, k-1, \\ a^{2^i q} \underset{(m)}{\not\equiv} -1 \end{array} \right\}.$$

The set L is precisely its complement in $(\mathbb{Z}/m\mathbb{Z})^*$: to see this, first suppose that $a \in M \cap L$, and derive a contradiction. (If $a^{2^k q} \underset{(m)}{\equiv} 1$, then $a \in L$ says we have to have $a^{2^{k-1} q} \underset{(m)}{\equiv} \pm 1$, while $a \in M$ says that the "-1" option is out; then $a^{2^{k-1} q} \underset{(m)}{\equiv} 1$ implies $a^{2^{k-2} q} \underset{(m)}{\equiv} \pm 1$, and so on, until we reach $a^q \underset{(m)}{\equiv} \pm 1$, which contradicts $a \in M$.) Then suppose $a \in (\mathbb{Z}/m\mathbb{Z})^*$ but $a \notin M$, and show $a \in L$ (left to you).

so that it suffices to show $|H| \leq \frac{1}{4}|G|$. Moreover

$$G = \left\{ \Theta(a_1, \ldots, a_r) \,\middle|\, a_j^{2^\ell q} \underset{(p_j)}{\equiv} 1 \,(\forall j) \right\}$$
$$= \left\{ \Theta(a_1, \ldots, a_r) \,\middle|\, a_j^{2^{\ell-1} q} \underset{(p_j)}{\equiv} \pm 1 \,(\forall j) \right\},$$

since p_j is prime.

So under the map $(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ which takes $(2^{\ell-1}q)^{\text{th}}$ powers, G is the preimage of of the 2^r elements $\Theta(\pm 1, \ldots, \pm 1)$. (These are all hit if you believe my claim that each $(\mathbb{Z}/p_j\mathbb{Z})^*$ has a generator,[6] a fact we'll see in §II.F.) On the other hand, H is the preimage of the two elements $1 = \Theta(1, \ldots, 1)$ and $-1 = \Theta(-1, \ldots, -1)$. Assuming the preimages of elements each have the same size (a general property of "group homomorphisms", discussed in §II.E), we see that

$$|H| \leq \frac{2}{2^r}|G| = \frac{1}{2^{r-1}}|G| \leq \frac{1}{4}|G|$$

since $r \geq 3$. □

If the conjecture alluded to above is true, then the Miller-Rabin test would determine whether m is prime or composite in "polynomial time" — that is, polynomial in $\log_2(m)$, roughly the number of binary digits of m. This would put (I) and (II)(a) (see the beginning of the section) in class

P :=class of decision problems solvable
by a polynomial-time algorithm.

It is actually easy to see that all 3 problems are in

NP :=class of decision problems whose solution
may be *verified* in polynomial time.

[6] and $2^{\ell-1}$ is a *proper* factor of 2^{k_j}, so that $p_j - 1$(=order of the generator) doesn't divide $2^{\ell-1}q$.

For (II)(a)-(b), suppose we are told a number m is composite, with prime factorization $p_1^{a_1} \cdots p_r^{a_r}$. To check this, you multiply, which proceeds digit by digit, hence in polynomial time... but we also need to check that the p_i are prime (so that (I) comes along for the ride too). Here, it's understood that you are given a "certificate" for the claim "the p_i are prime": this would consist of a **generator** of $(\mathbb{Z}/p_i\mathbb{Z})^*$, i.e. an α for which $\alpha^{p_i-1} \underset{(p_i)}{\equiv} 1$ but $\alpha^{\frac{p_i-1}{q}} \underset{(p_i)}{\not\equiv} 1$ for any prime $q|(p_i - 1)$. (Such an element exists exactly when p_i is prime.) This can be checked using fast-powering in polynomial time, *assuming* you are also given a prime factorization for $p_i - 1$, with necessary certificates, and so on. We conclude that

$$\text{(I),(II)(a),(II)(b)} \in \mathbf{NP}.$$

Now, it is still not known whether (II)(b) belongs to **P**; in fact, it is hoped that it does not, so that factoring is hard (and public key cryptography secure!). On the other hand, we have the

(6) AKS primality test, which implies that

$$\text{(I),(II)(a)} \in \mathbf{P}!!$$

We state the test as

THEOREM 94 (Agrawal-Kayal-Saxena, 2002). *Let $r \in \mathbb{Z} \cap [2, m)$ be such that m has order $> (\log_2 m)^2$ mod r. Then*[7]

$$m \text{ is prime} \iff \begin{cases} \textit{(i)} & m \textit{ is not a perfect power,} \\ \textit{(ii)} & m \textit{ has no prime factor} \leq r, \textit{ and} \\ \textit{(iii)} & (x+a)^m \equiv x^m + a \bmod (m, x^r - 1) \\ & \textit{for each } a \in \mathbb{Z} \cap [1, \sqrt{r}\log_2 m]. \end{cases}$$

A key point in their paper (which is short, and readable with basic knowledge of group and ring theory) is that we can take $r < \lceil (\log_2 m)^5 \rceil$. This is what gives the polynomial time, since you only have to check the first r coefficients of $(x+a)^m - x^m - a$ are zero

[7] See the exercises for how to check (i) in polynomial time.

mod m (for each $a \in \mathbb{Z} \cap [1, \sqrt{r}\log_2 m]$); but note that m only surpasses $(\log_2 m)^5$ at $m_0 = 5,690,034$. Up to this m_0, the algorithm is just a brute force "check for factors", making Miller-Rabin much more suitable for "domestic use".

One direction (namely, " $\implies$ ") in the Theorem is easy; in fact, we will prove a bit more:

PROPOSITION 95. *Let $a \in \mathbb{Z}$ be coprime to m. Then m is prime if and only if*

$$(x+a)^m \underset{(m)}{\equiv} x^m + a. \tag{20}$$

PROOF. If $m = p$ is prime, then $a^p \underset{(p)}{\equiv} a$ (Fermat) and

$$\binom{p}{k} = \tfrac{p(p-1)\cdots(p-k+1)}{k!} \underset{(p)}{\equiv} 0.$$

So

$$(x+a)^p = x^p + \sum_{k=1}^{p-1}\binom{p}{k}x^k a^{p-k} + a^p \underset{(p)}{\equiv} x^p + a,$$

and we're done.

If m is composite, consider a prime factor q, with $\mathrm{ord}_q(m) = k$ (i.e. $m = q^k w$ with $(q,w) = 1$). Then we have

$$q^k \nmid \binom{m}{q} = \frac{m(m-1)\cdots(m-q+1)}{q!},$$

and $a^{m-q} = (a^{w-1})^q \underset{(q)}{\equiv} 1 \implies (q^k, a^{m-q}) = 1$; so the coefficient of x^q in $f(x) = (x+a)^m - x^m - a$ is not divisible by q^k. Since $q^k | m$, it isn't divisible by m, and so neither is $f(x)$. □

Pollard rho method. The methods we have been describing for showing m is prime or composite don't find us a factor in general. As we mentioned, the factoring problem (II)(b) is expected to be harder (not in **P**). But there are still some useful algorithms, one of which (due to J. Pollard in 1975) we now describe.

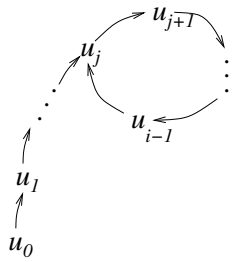
Let m be a *known composite*, $u_0 \in \mathbb{Z}/m\mathbb{Z}$, and use $f(n) := u^2 + c$ ($c \in \mathbb{Z}$, say $c = 1$) to recursively generate a sequence by $u_{i+1} :\underset{(m)}{\equiv}$

$f(u_i)$. If the smallest prime factor of m is p, then one expects (to high probability) at least one of the numbers

$$d_s := (u_{2s} - u_s, m), \quad s = 1, \ldots, 2\lceil\sqrt{p}\rceil$$

to be distinct from 1 and m, hence yielding a proper factor of m.

Why does one expect this? The idea is that $2\lceil\sqrt{p}\rceil$ numbers are likely not to be distinct mod p (this is related to the birthday problem), but distinct mod m. Hence some $u_i - u_j$ should be divisible by p but not by m, and then $p|(u_i - u_j, m) \neq m$. Moreover, $u_i \underset{(p)}{\equiv} u_j \implies u_{i+1} = f(u_i) \underset{(p)}{\equiv} f(u_j) = u_{j+1} \implies \{u_i\}$ periodic mod p with period $r = i - j$ (after some point). This is why we only need to check differences of the form $u_{2s} - u_s$. The name of the method comes from the similarity of the shape in the figure (which depicts the $\{u_i\}$ mod p) to the Greek letter ρ:



EXAMPLE 96. Let $m = 1729$ (which is a Carmichael number), $f(u) = u^2 + 1$, and $u_0 = 1$. Working mod m, we get

$$u_i = 1,\ 2,\ 5,\ 26,\ 677,\ 145,\ 278.$$

We have $u_2 - u_1 = 3 \implies d_1 = 1$, but then

$$u_4 - u_2 = 672 \implies d_2 = 7.$$

So $m = 7 \cdot 247 = 7 \cdot 13 \cdot 17$.

Exercises

(1) Let $m = 11111$. Show that $2^{m-1} \underset{(m)}{\equiv} 10536$. Deduce that m is composite.

(2) Prove that $1729 = 7 \cdot 13 \cdot 19$ and $10585 = 5 \cdot 29 \cdot 73$ are Carmichael numbers.

(3) So, Wilson's theorem said that if m is prime, then $(m-1)! \underset{(m)}{\equiv} -1$. Check that the converse holds: i.e. that if m is composite then the congruence fails. (Of course, this is terribly inefficient as a primality test.)

(4) Apply the Miller-Rabin test to 2773. Is it composite or "likely prime"?

(5) 8051 is composite. Factor it using Pollard's ρ method.

(6) Devise a test that will decide in polynomial time whether a given $n \in \mathbb{N}$ is a perfect power, i.e., of the form a^b (where $a, b \in \mathbb{N}$). (You will recall that "polynomial" essentially means bounded by a constant times a power of $\log(n)$.)

(7) Let X be a large positive integer. Suppose that $m \leq X/2$, and that $0 \leq a < m$, $0 \leq b < m$. Explain why the number c determined by the following algorithm satisfies $0 \leq c < m$, and $c \underset{(m)}{\equiv} ab$. Verify that in executing the algorithm, all numbers encountered lie in the interval $[0, X)$.

1. Set $k = b$, $c = 0$, $g = \left\lfloor \frac{X}{m} \right\rfloor$.

2. As long as $a > 0$, perform the following operations:

(a) Set $r = a - g \left\lfloor \frac{a}{g} \right\rfloor$.

(b) Choose s so that $s \underset{(m)}{\equiv} kr$ and $0 \leq s < m$.

(c) Replace c by $c + s$.

(d) If $c \geq m$, replace c by $c - m$.

(e) Replace k by $gk - m \left\lfloor \frac{gk}{m} \right\rfloor$.

(f) Replace a by $\frac{a-r}{g}$.

CHAPTER 9

Groups, rings, and fields

As suggested by the proof of Theorem II.D.10 and the discussion of "certificates for primeness" in the last section, it will be helpful to know a bit about these three basic structures in abstract algebra. In fact, it will turn out that we already have several examples, and that these structures give an efficient framework for thinking about them.

DEFINITION 97. A **group** is a set G with a binary operation, which is to say a mapping

$$\bullet : G \times G \to G,$$

such that:

(i) $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ $(\forall x, y, z \in G)$ [associativity]

(ii) G has an element "1" with $1 \bullet x = x = x \bullet 1$ $(\forall x \in G)$

(iii) for each $x \in G$, $\exists$"x^{-1}"$\in G$ with $x^{-1} \bullet x = 1 = x \bullet x^{-1}$

If you omit (iii) (existence of inverses), then G is a **monoid**.

We write $|G|$ for the number of elements, called the **order** of G, and call G **abelian** (or commutative) if $x \bullet y = y \bullet x$ $(\forall x, y \in G)$. In the latter case, one sometimes writes "$+$" and "0" instead of "$\bullet$" and "1".[1]

Abelian examples: Infinite order:

- $(\mathbb{Z}, +)$, the **infinite cyclic** group, *generated* by 1. (This means that repeatedly adding 1 and its inverse -1 gives all the elements in the group.)
- $(\mathbb{Q}^*, \cdot\,)$ (where $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$).

[1] In the sequel, "$\bullet$" will be usually be addition ("$+$") or multiplication ("$\cdot$"). Sometimes $a \cdot b$ will just be written ab.

Finite order:

- $(\mathbb{Z}/m\mathbb{Z}, +)$ the **finite cyclic group** of order m, *generated* by 1.
- $((\mathbb{Z}/m\mathbb{Z})^*, \cdot\,)$, which has order $\phi(m)$.

Nonabelian examples: Infinite order:

- $(SL_2(\mathbb{Z}), \text{matrix mult.})$, the group of 2×2 matrices with integer entries and determinant 1.

To see the noncommutativity, consider the products

$$\begin{pmatrix} a & \\ & b \end{pmatrix}\begin{pmatrix} & 1 \\ 1 & \end{pmatrix} = \begin{pmatrix} & a \\ b & \end{pmatrix} \neq \begin{pmatrix} & b \\ a & \end{pmatrix} = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}\begin{pmatrix} a & \\ & b \end{pmatrix}.$$

Finite order:

- $(\mathcal{S}_n, \circ)$, the **symmetric group** of permutations of $\{1, \ldots, n\}$ with composition of permutations "$\circ$" as its binary operation; this has order $n!$
- $(D_n, \circ)$, the **dihedral group** of rotational and reflectional symmetries of a regular n-gon; it has order $2n$.

Further examples may be constructed by taking *direct products*: given groups G_1 and G_2, $G_1 \times G_2$ is the group with elements (g_1, g_2), identity $(1, 1)$, and product $(g_1, g_2) \bullet (g_1', g_2') = (g_1 g_1', g_2 g_2')$.

Basic properties: in a group G,

- the cancellation laws hold: $xa = xb$ or $ax = bx \implies a = b$; hence
- inverses are unique, and $(x^{-1})^{-1} = x$;
- $(ab)^{-1} = b^{-1}a^{-1}$;
- $(a^n)^m = a^{nm}$, $a^n a^m = a^{n+m}$ (where $a^n := \underbrace{a \bullet \cdots \bullet a}_{n \text{ times}}$);
- *if* $ab = ba$, then $(ab)^n = a^n b^n$.

DEFINITION 98. A **subgroup** of G is a subset $H \subseteq G$ satisfying:
(i) $1 \in H$;
(ii) $x, y \in H \implies xy \in H$; and
(iii) $x \in H \implies x^{-1} \in H$.

Subgroups are, of course, groups; we write $H \leq G$. The **cyclic subgroup** generated by $g \in G$ is

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\} \leq G.$$

Define the **order** of g by

$$\mathrm{ord}(g) := |\langle g \rangle|.$$

PROPOSITION 99. *If $\mathrm{ord}(g)$ is finite, it is the smallest power $k \in \mathbb{N}$ for which $g^k = 1$. (Otherwise, $g^k \neq 1$ for every $k \in \mathbb{N}$.)*

PROOF. Assume $k = \mathrm{ord}(g) < \infty$. Then $1, g, g^2, \ldots, g^{k-1}$ is a complete list of the elements of $\langle g \rangle$. If $g^j = g^i$ for distinct $i, j \in \{0, 1, \ldots, k-1\}$, then $g^{|j-i|} = 1$ contradicting minimality of k. □

Examples of subgroups:

- in any group, the "trivial" subgroup $\{1\}$;
- in $(\mathbb{Z}, +)$, $\langle 2 \rangle = 2\mathbb{Z}$;
- in $(\mathbb{C}^*, \cdot)$, $\langle e^{\frac{2\pi i}{n}} \rangle$ is a cyclic group (of order n);
- all finite groups "appear" as subgroups in some $\mathcal{S}_n$ (idea: the group permutes its own elements);
- intersections of subgroups are subgroups.

THEOREM 100 (Langrange). *Given $H \leq G$ with $|G| < \infty$, $|H|$ divides $|G|$.*

LEMMA 101. *Distinct **cosets** $gH := \{gh \mid h \in H\} \subseteq G$ of H are disjoint, and have the same number of elements.*

PROOF. First observe that

$$\begin{aligned} a \in bH &\iff b^{-1}a \in H \text{ (and } a^{-1}b \in H) \\ &\iff b^{-1}aH \subset H \text{ and } a^{-1}bH \subset H \\ &\iff aH \subset bH \text{ and } bH \subset aH \\ &\iff aH = bH. \end{aligned}$$

Suppose $aH \neq bH$. Given $\alpha \in aH$, $\alpha H = aH \neq bH \implies \alpha \notin bH$. So $aH \cap bH = \emptyset$.

Finally, the map $H \to aH$ sending $a \mapsto ah$ is a bijection, by the cancellation law. □

PROOF OF LANGRANGE'S THEOREM. By the Lemma, $G = a_1H \amalg \cdots \amalg a_rH$ (disjoint union), and each $|a_iH| = |H|$. □

Easy consequences of Lagrange:

- $\mathrm{ord}(g) \mid |G|$ for any $g \in G$ (in particular, $g^{|G|} = 1$); hence
- immediate proof of Fermat/Euler by taking $G = (\mathbb{Z}/m\mathbb{Z})^*$; and
- any group of prime order is cyclic (why?).

For another consequence, related to §II.D, we need the important

DEFINITION 102. (i) A (group) **homomorphism** is a map of groups

$$\varphi : G \to H$$

respecting the binary operation:

$$\varphi(xy) = \varphi(x)\varphi(y) \quad (\forall x, y \in G). \tag{21}$$

Note that (21) $\implies \varphi(1) = 1$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$. (Why?)

(ii) If a homomorphism φ is 1-to-1 and onto, it is called an **isomorphism** and the groups are said to be **isomorphic**, i.e. "the same"[2] from the standpoint of group structure; we write $G \cong H$.

(iii) The **kernel** and **image** of φ are

$$\ker(\varphi) := \{g \in G \,|\, \varphi(g) = 1\} \subset G$$
$$\mathrm{im}(\varphi) := \{\varphi(g) \,|\, g \in G\} \subset H.$$

Note that if φ is an isomorphism, $\ker(\varphi) = \{1\}$ and $\mathrm{im}(\varphi) = H$.

PROPOSITION 103. *(i)* $\ker(\varphi) \leq G$ *and (ii)* $im(\varphi) \leq H$.

PROOF OF (I). $\varphi(g) = 1 = \varphi(g') \implies \varphi(gg') = \varphi(g)\varphi(g') = 1 \cdot 1 = 1$. □

[2] e.g. same order, same order of elements, etc.

Given $k \in \ker(\varphi)$, $\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g) \cdot 1 = \varphi(g)$, so the cosets of $\ker(\varphi)$ are the preimages $\varphi^{-1}(h)$ of $h \in \mathrm{im}(\varphi)$. Together with Lemma 101, this gives the

COROLLARY 104. *Given a homomorphism $\varphi : G \to H$, the preimages $\varphi^{-1}(h)$ of $h \in im(\varphi)$ all have the same number of elements.*

In §II.F, we will delve into the structure of the group $(\mathbb{Z}/m\mathbb{Z})^*$. In the remainder of this section, we shall briefly explicate another basic structure:

DEFINITION 105. A ring is a set R together with two binary operations $(+, \cdot)$ and two distinguished elements $0, 1 \in R$, satisfying:

(i) $(R, +, 0)$ is an abelian group;

(ii) $(R, \cdot, 1)$ is a monoid;

(iii) distributivity: $r \cdot (s_1 + s_2) = r \cdot s_1 + r \cdot s_2$, $(r_1 + r_2) \cdot s = r_1 \cdot s + r_2 \cdot s$ ($\implies 0 \cdot r = 0$)

In the same way as in Definitions 98 and 102, one may define subrings, direct products, homomorphisms (respecting both "$+$" and "$\cdot$"), and isomorphisms of rings.

Examples:

- $M_2(\mathbb{Z})$, the ring of 2×2 matrices with integer entries. (Here "$\cdot$" is not commutative. Usually we'll only work with commutative rings.)
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/m\mathbb{Z}$
- $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ ($d \in \mathbb{Z}$ squarefree)
- $\mathbb{Z}[x]$ = polynomials with integer coefficients[3]

Inside any ring R, the set of **units** (elements with multiplicative inverses) forms a group under multiplication, denoted R^*.

Examples:

- $(\mathbb{Z}/m\mathbb{Z})^*$
- $\mathbb{Z}^* = \{1, -1\}$

[3]More generally, given any commutative ring R, we can consider the ring $R[x]$ of polynomials with coefficients in R.

- $M_2(\mathbb{Z})^* = 2 \times 2$ matrices with determinant ± 1.

Consider $\mathbb{Z}/6\mathbb{Z}$: we have $2 \cdot 3 \underset{(6)}{\equiv} 0$, making it impossible for 2 or 3 (or 4) to have inverses. Indeed, the units are just $(\mathbb{Z}/6\mathbb{Z})^* = \{1, -1\}$.

Here is a particularly nice type of ring:

DEFINITION 106. A **field** is a commutative ring with $R^* = R \backslash \{0\}$, i.e. all nonzero elements are units.

Examples:

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (but not $\mathbb{Z}$)
- $\mathbb{Q}[\sqrt{d}] = \{p + q\sqrt{d} \mid p, q \in \mathbb{Q}\}$ (Why?)

THEOREM 107. *$\mathbb{Z}/m\mathbb{Z}$ is a field $\iff$ m is a prime.*

PROOF. ($\implies$) If $m = n_1 n_2$ (both $n_i > 1$), then $n_1 \cdot n_2 \underset{(m)}{\equiv} 0 \implies$ n_1, n_2 not invertible.

($\impliedby$) If $m = p$ is a prime, then any nonzero residue class n is prime to p. So we have $x, y \in \mathbb{Z}$ such that $nx + py = 1$, and thus $nx \underset{(p)}{\equiv} 1$. □

One last thing to notice is that the Chinese Remainder Theorem is really a statement about an isomorphism of rings: if $(m, n) = 1$ then

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

The group isomorphism

$$(\mathbb{Z}/mn\mathbb{Z})^* \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

follows by taking unit groups on both sides.

Exercises

(1) Let d be a nonzero integer. Show that the ring $\mathbb{Q}[\sqrt{d}] := \{q_1 + q_2\sqrt{d} \mid q_1, q_2 \in \mathbb{Q}\}$ is in fact a field.
(2) Show that there are essentially (i.e. up to isomorphism) only two groups of order 4. [Hint: start by considering what are the possible orders of elements, keeping in mind only the identity "1" has order 1.]

(3) Which of the following groups are isomorphic: $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, $(\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, $\mathbb{Z}/24\mathbb{Z}$, $\mathcal{S}_4$?

CHAPTER 10

Primitive roots

Let p be a prime. By Theorem II.E.11, $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ is a (finite) field, and $(\mathbb{F}_p^*, \cdot\,)$ an abelian group of order $p-1$. Of what kind? To determine this, we begin by considering the **polynomial ring**

$$\mathbb{F}_p[x] := \{\underbrace{a_0 + a_1 x + \cdots + a_n x^n}_{\text{elements ``}f\text{'' or ``}f(x)\text{''}} \mid n \in \mathbb{Z}_{\geq 0},\ a_i \in \mathbb{F}_p\}.$$

The **degree** of a polynomial $f \in \mathbb{F}_p[x]\backslash\{0\}$ is the largest n for which $a_n \neq 0$ (in $\mathbb{F}_p$; i.e. $a_n \underset{(p)}{\not\equiv} 0$). We have $\deg(fg) = \deg(f) + \deg(g)$.

Division algorithm for $\mathbb{F}_p[x]$: Given $f, g \in \mathbb{F}_p[x]$, polynomial long division yields $q, r \in \mathbb{F}_p[x]$ such that

$$f = gq + r \quad \text{in } \mathbb{F}_p[x]$$

and

$$\deg(r) < \deg(g) \ \text{ or } \ r = 0.$$

(Here and in what follows, coefficients are considered modulo p; since we are working in $\mathbb{F}_p[x]$ and $\mathbb{F}_p$ "=" will mean "$\underset{(p)}{\equiv}$".) We write $g \mid f \iff gq = f$ in $\mathbb{F}_p[x]$, for some $q \in \mathbb{F}_p[x]$.

THEOREM 108. *Let $f \in \mathbb{F}_p[x]$ and $a \in \mathbb{F}_p$. Then $f(a) = 0 \implies (x-a) \mid f(x)$.*

PROOF. By the division algorithm, $f = (x-a)q + r$ where $\deg(r) = 0$ or $r = 0$, i.e. $r \in \mathbb{F}_p$. So

$$0 = f(a) = (a-a)q(a) + r = r.$$

□

COROLLARY 109. *Let $F \in \mathbb{Z}[x]$ be a polynomial, and $F_p \in \mathbb{F}_p[x]$ its "reduction modulo p". Assume $F_p \neq 0$ of degree n_p. Then the congruence $F(x) \underset{(p)}{\equiv} 0$ has at most n_p distinct solutions in $\mathbb{F}_p$.*

PROOF. Let $a_1, \ldots, a_n \in \mathbb{F}_p$ be distinct solutions. Then in $\mathbb{F}_p[x]$, $(x - a_1) \mid F_p \implies F_{p,1} := \frac{F_p}{(x-a)} \in \mathbb{F}_p[x]$ has $a_2, \ldots, a_n$ as roots, so $(x - a_2) \mid F_{p,1}$ and so on. So we get

$$F_p = g \cdot \prod_{i=1}^{n} (x - a_i)$$

and hence $n_p \geq n$. □

EXAMPLE 110. (i) $3x^4 + x^2 - 1 \underset{(3)}{\equiv} 0$ can have at most 2 distinct solutions (mod 3), because (writing $F(x) = 3x^4 + x^2 - 1$) we have $F_3 = x^2 - 1$. The two solutions are ± 1.

(ii) $x^p - x - 1 \underset{(p)}{\equiv} 0$ has *no* solutions (mod p) by little Fermat.

COROLLARY 111. *Let $f \in \mathbb{F}_p[x]$ be of degree n. Then $f(x) = 0$ has n solutions in $\mathbb{F}_p \iff f \mid (x^p - x)$ in $\mathbb{F}_p[x]$.*

PROOF. By Theorem 108 and little Fermat, $x^p - x = \prod_{k=0}^{p-1} (x - k)$ (in $\mathbb{F}_p[x]$); and by Theorem 108, f (of degree n) has n roots iff $f(x) = a \prod_{\ell=1}^{n} (x - k_\ell)$, with $a \in \mathbb{F}_p^*$ and $k_1, \ldots, k_n \in \mathbb{F}_p$ distinct. □

COROLLARY 112. *If $d \mid p - 1$, then $x^d \underset{(p)}{\equiv} 1$ has d solutions.*

PROOF. Writing $p - 1 = de$, $(y - 1)(1 + y + y^2 + \cdots + y^{e-1}) = y^e - 1 \implies x^p - x = x(x^{de} - 1) = x(x^d - 1)(1 + x^d + x^{2d} + \cdots + x^{(e-1)d})$. Apply Corollary 111. □

This is the extent to which we shall need to use polynomial rings for now. Turning to groups, we summarize the basic rules governing orders of elements. Let $g \in G$ have order n. (Recall that this is the smallest power of g that gives 1.)

(i). $n \mid |G|$ (by Lagrange).

(ii). $g^k = 1 \iff n \mid k$.

[Write $k = qn + r$ with $0 \leq r < n$, then $1 = (g^n)^q g^r = g^r \iff r = 0$.]

(iii). $\mathrm{ord}(g^a) = \frac{n}{(n,a)}$,

which gives the orders of all elements of $\langle g \rangle$. [By **(ii)**, $1 = (g^a)^m \iff n \mid am \iff \frac{n}{(n,a)} \mid \frac{a}{(n,a)}m \iff \frac{n}{(n,a)} \mid m$.]

(iv). If h has order m coprime to n, and $hg = gh$, then $\mathrm{ord}(gh) = mn$.

[$(gh)^{mn} = (g^n)^m (h^m)^n = 1$; and $1 = (gh)^a = g^a h^a \implies g^a = h^{-a} \implies g^{am} = (h^m)^{-a} = 1 \implies n \mid am \implies n \mid a$. Similarly $m \mid a$ so $mn \mid a$. Done by **(ii)**.]

Recall that (by **(i)**) in the group $(\mathbb{Z}/m\mathbb{Z})^*$, orders of elements *divide* $\phi(m)$.

DEFINITION 113. A primitve root modulo m is a residue class $g \in (\mathbb{Z}/m\mathbb{Z})^*$ with $\mathrm{ord}(g) = \phi(m)$.

The following is immediately clear:

PROPOSITION 114. *If a primitive root mod m exists, then $(\mathbb{Z}/m\mathbb{Z})^*$ is a cyclic group of order $\phi(m)$; more precisely, we have an isomorphism*

$$\begin{array}{ccc} (\mathbb{Z}/\phi(m)\mathbb{Z}, +) & \xrightarrow{\cong} & ((\mathbb{Z}/m\mathbb{Z})^*, \cdot\,). \\ a & \longmapsto & g^a \end{array}$$

EXAMPLE 115. (a) In $(\mathbb{Z}/7\mathbb{Z})^* = \{1,2,3,4,5,6\}$, $2^3 \underset{(7)}{\equiv} 1$ and so 2 is not a primitive root. Try 3 next: modulo 7, we have

$$3 \overset{\cdot 3}{\to} 2 \overset{\cdot 3}{\to} 6 \overset{\cdot 3}{\to} 4 \overset{\cdot 3}{\to} 5 \overset{\cdot 3}{\to} 1,$$

and thus 3 is a primitive root. Since a primitive root mod 7 exists, we have $(\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$.

(b) In $(\mathbb{Z}/8\mathbb{Z})^*\{1,3,5,7\}$, we have $3 \cdot 3 \underset{(8)}{\equiv} 1$, $5 \cdot 5 \underset{(8)}{\equiv} 1$, $7 \cdot 7 \underset{(8)}{\equiv} 1$ $\implies$ no primitive roots mod 8. We have $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the "Klein 4-group".

It turns out that

$$\textit{primitive roots mod } m \textit{ exist for } m = 2, 4, p^r, 2p^r$$

where p is any odd prime and $\alpha \geq 1$. We will prove the odd prime case now.[1] (Let p be an odd prime.)

LEMMA 116. *Given a prime power divisor $q^r \mid p-1$, there are $q^r - q^{r-1}$ elements of $\mathbb{F}_p^*$ with order q^r.*

PROOF. By Corollary 112, $x^{q^r} = 1$ [resp. $x^{q^{r-1}} = 1$] has q^r [resp. q^{r-1}] solutions in $\mathbb{F}_p^*$. The divisors of q^r are q^r and divisors of q^{r-1}, so by **(ii)** we are done. □

THEOREM 117. *There are $\phi(p-1)$ primitive roots mod p. In particular, $\mathbb{F}_p^*$ is cyclic.*

PROOF. Write $p - 1 = \prod q_i^{r_i}$, with q_i distinct primes. By the Lemma, we have (for each i) elements $g_i \in \mathbb{F}_p^*$ of order $q_i^{r_i}$, hence by **(iv)** $g := \prod g_i^{r_i}$ has order $\prod q_i^{r_i} = p - 1$. So $\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$, and g^k has order $p - 1 \underset{\textbf{(iii)}}{\iff} (p-1, k) = 1$. □

REMARK 118. We can use Theorem 117 to aid in the construction of large primes. Set $M := \prod p_i + 1$, for p_i small distinct primes. If Miller-Rabin shows M is a very likely prime, then prove M is prime by exhibiting an element of order $M - 1$:[2] pick small $g \geq 2$, and show $g^{\frac{M-1}{p_i}} \underset{(M)}{\not\equiv} 1$ for each i.

According to a conjecture of E. Artin, $g = 2$ should generate $\mathbb{F}_p^*$ for infinitely many p, but this is still an open (and very difficult) problem.

Exercises

(1) Prove that if m is a Carmichael number, then it is of the form $p_1 \cdot \cdots \cdot p_k$, where p_i are distinct primes with $p_i - 1 | m - 1$. You

[1] The cases $m = 2, 4$ are trivial, and we will do p^r for $r > 1$ in the next section. For $2p^r$, see [NZM] §2.8.

[2] As mentioned above, there are a few types of composite M for which $(\mathbb{Z}/M\mathbb{Z})^*$ has a primitive root, but in that case the order is $\phi(M) < M - 1$.

may use that m is odd. [Hint: a priori, $m = \prod p_i^{r_i}$ for some odd primes p_i. Use the Chinese remainder theorem together with a result on primitive roots.]

(2) Look back at problem (3) from the previous Chapter. What about $\mathbb{Z}_{35}^*$?

(3) Use Corollary 111 to solve $2x^3 + 5x^2 + 6x + 1 \underset{(7)}{\equiv} 0$.

(4) Show that $3^8 \underset{(17)}{\equiv} -1$, and explain why this implies that 3 is a primitive root mod 17.

(5) Without finding them, how many solutions (if any) does $x^{20} \underset{(17)}{\equiv} 13$ have?

CHAPTER 11

Prime power moduli and power residues

In §II.C, we used the Chinese Remainder Theorem to reduce congruences modulo $m = \prod p_i^{r_i}$ to congruences modulo $p_i^{r_i}$. For examples and problems, we stuck with $r_i = 1$ because we had no techniques to reduce from "mod $p_i^{r_i}$" to "mod p_i". We now discuss one approach to this.[1]

Let p be a prime, $f \in \mathbb{Z}[x]$ a polynomial.

THEOREM 119 (Hensel's Lemma). *Let $\alpha \in \mathbb{Z}/p^j\mathbb{Z}$ be a solution of $f(x) \underset{(p^j)}{\equiv} 0$, with $f'(\alpha) \underset{(p)}{\not\equiv} 0$. Then there exists a unique solution $\tilde{\alpha} \in \mathbb{Z}/p^{j+1}\mathbb{Z}$ of $f(x) \underset{(p^{j+1})}{\equiv} 0$, with $\tilde{\alpha} \underset{(p^j)}{\equiv} \alpha$. We say that $\tilde{\alpha}$ "lifts" α.*

PROOF. Let a be an integer reducing to α mod p^j, so that $f(a) \underset{(p^j)}{\equiv} 0$. Writing $n = \deg(f)$, consider the "Taylor" expansion

$$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \cdots + t^n p^{nj} \frac{f^{(n)}(a)}{n!},$$

where the $\frac{f^{(k)}(a)}{k!}$ are integers. (Why?[2]) Reducing mod p^{j+1}, we have

$$f(a + tp^j) \underset{(p^{j+1})}{\equiv} f(a) + tp^j f'(a);$$

and so t solves $f(a + tp^j) \underset{(p^{j+1})}{\equiv} 0$

$$\iff \quad t \text{ solves } tp^j f'(a) \underset{(p^{j+1})}{\equiv} -f(a)$$

$$\underset{(f(a) \underset{(p^j)}{\equiv} 0)}{\iff} \quad t \text{ solves } tf'(a) \underset{(p)}{\equiv} -\frac{f(a)}{p^j}$$

[1] If you want to know more, see [NZM] §2.6.

[2] Hint: the $\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!}$ are integers for each $m \geq k$.

$$\underset{(f'(a)\not\equiv 0 \pmod{p})}{\Longleftrightarrow} \quad t \underset{(p)}{\equiv} -\frac{f(a)}{p^j f'(a)}.$$

This uniquely specifies the congruence class $\tilde{\alpha}$ of $a + tp^j$ modulo p^{j+1}. □

EXAMPLE 120. ($p \neq 2$) Let $m \in \{1, 2, \ldots, p-1\}$. When does $x^2 \underset{(p^n)}{\equiv} m$ have a solution? That is, when does m have a "square root" in $\mathbb{Z}/p^n\mathbb{Z}$?

Clearly $x^2 \underset{(p^n)}{\equiv} m \implies x^2 \underset{(p)}{\equiv} m$, so m must be a square mod p (which is true for half of $\{1, 2, \ldots, p-1\}$). Suppose this is true: $m \underset{(p)}{\equiv} a_1^2$, i.e. $f(a_1) := a_1^2 - m \underset{(p)}{\equiv} 0$. Then we have the base case for the following induction: if $f(x) \underset{(p^j)}{\equiv} 0$ has a solution a_j (lifting a_1), then

$$f'(a_j) = 2a_j \underset{(p)}{\not\equiv} 0 \ \text{ (since } a_j \underset{(p)}{\equiv} a_1 \underset{(p)}{\not\equiv} 0, \text{ and } 2 \underset{(p)}{\not\equiv} 0),$$

so Hensel implies the existence of an a_{j+1} (lifting a_j hence a_1) such that $f(a_{j+1}) \underset{(p^{j+1})}{\equiv} 0$. Conclude that

$$\sqrt{m} \text{ exists in } \mathbb{Z}/p^n\mathbb{Z} \iff \sqrt{m} \text{ exists in } \mathbb{Z}/p\mathbb{Z}.$$

For instance, if $m = 2$ and $p = 7$, $a_1^2 \underset{(7)}{\equiv} 2 \implies a_1 = 3$ or 4, say 3. Now to construct a square root mod 7^2 we set

$$\begin{aligned} 2 \underset{(7^2)}{\equiv} \underbrace{(3 + 7t_1)}_{=:a_2}{}^2 \underset{(7^2)}{\equiv} 9 + 42t_1 &\implies 42t_1 \underset{(7^2)}{\equiv} -7 \\ &\implies 6t_1 \underset{(7)}{\equiv} -1 \implies t_1 = 1 \\ &\implies a_2 = 10 \end{aligned}$$

then to lift mod 7^3

$$2 \underset{(7^3)}{\equiv} (\underbrace{10 + 7^2 t_2}_{=:a_3})^2 \underset{(7^3)}{\equiv} 100 + 294t_2 \implies 294t_2 \underset{(7^3)}{\equiv} -98$$
$$\implies 6t_2 \underset{(7)}{\equiv} -2 \implies t_2 = 2$$
$$\implies a_3 = 108$$

and so on.

So you see that in this case a congruence problem for p^n got reduced to one mod p.

We now use Hensel's Lemma to deal with primitive roots. Here p will be an odd prime.

Step 1 (mod p^2): Let[3] g be a primitive root mod p, and $t \in \mathbb{Z}/p\mathbb{Z}$. Then $(g + tp, p) = (g, p) = 1 \implies (g + tp, p^2) = 1 \implies g + tp$ belongs to $(\mathbb{Z}/p^2\mathbb{Z})^*$. Denote its order by h, and note that $h \mid |(\mathbb{Z}/p^2\mathbb{Z})^*| = \phi(p^2) = p(p-1)$. Moreover, $(g + tp)^h \underset{(p^2)}{\equiv} 1 \implies g^h \underset{(p)}{\equiv} (g + tp)^h \underset{(p)}{\equiv} 1$, which by Fermat (and the fact that g generates $(\mathbb{Z}/p\mathbb{Z})^*$) gives $(p-1) \mid h$. So $h = p-1$ or $p(p-1)$. Now set $f(x) := x^{p-1} - 1$, $\alpha = g$, and note $f'(g) = (p-1)g^{p-2} \underset{(p)}{\not\equiv} 0$. By Hensel's Lemma, there is a unique solution of $f(x) \underset{(p^2)}{\equiv} 0$, i.e. a unique choice of t so that $h = p-1$. So for other choices, $h = p(p-1)$ and $g + tp$ is a primitive root mod p^2.

Step 2 (mod $p^{r>2}$): Let g be a primitive root mod p^2; denote the order of g mod p^r by h_r, which must satisfy $h_r \mid \phi(p^r) = p^{r-1}(p-1)$ by Lagrange. Moreover, $g^{h_r} \underset{(p^r)}{\equiv} 1 \implies g^{h_r} \underset{(p^2)}{\equiv} 1 \implies p(p-1) \mid h_r$ (since g is primitive mod p^2) $\implies h_r = p^\beta(p-1)$ with $\beta \in \{1, \ldots, r-1\}$. We claim that $\beta = r-1$, i.e. $g^{p^{r-2}(p-1)} \underset{(p^r)}{\not\equiv} 1$ (for each $r \geq 2$).

[3]More precisely: g is some integer whose congruence class mod p generates $(\mathbb{Z}/p\mathbb{Z})^*$. Same thing at the beginning of Step 2 (with p^2 replacing p).

Since we know this for $r = 2$, assume it inductively for $2, \dots, r$ and prove for "$r+1$". That is, by assumption, $g^{p^{r-2}(p-1)}$ is $\underset{(p^{r-1})}{\equiv} 1$ but $\underset{(p^r)}{\not\equiv} 1$, so that we may write

$$g^{p^{r-2}(p-1)} = 1 + tp^{r-1}, \quad p \nmid t.$$

Taking p^{th} powers gives

$$g^{p^{r-1}(p-1)} = (1+tp^{r-1})^p = 1 + \binom{p}{1} tp^{r-1} + \left\{ \binom{p}{2} t^2 p^{2(r-1)} + \cdots \right\},$$

and since for $k \geq 2$ $p^{r+1} \mid \binom{p}{k} p^{k(r-1)}$ the bracketed terms die mod p^{r+1}, leaving us with

$$g^{p^{r-1}(p-1)} \underset{(p^{r+1})}{\equiv} 1 + tp^r \underset{(p^{r+1})}{\not\equiv} 1.$$

This proves the existence part of

THEOREM 121. *There exist $p^{r-2}(p-1)\phi(p-1)$ primitive roots mod p^r (p any odd prime, $r \geq 1$). In particular, $(\mathbb{Z}/p^r\mathbb{Z})^*$ is cyclic.*

PROOF. Existence of a single primitive root (done above) proves cyclicity, i.e. that $((\mathbb{Z}/p^r\mathbb{Z})^*, \cdot) \cong (\mathbb{Z}/\phi(p^r)\mathbb{Z}, +)$. Recalling that the order of m in $(\mathbb{Z}/n\mathbb{Z}, +)$ is $\frac{n}{(n,m)}$, so that m is a generator iff $(m,n) = 1$, we see that there are

$$\phi(\phi(p^r)) = \phi(p^{r-1}(p-1)) = \phi(p^{r-1})\phi(p-1) = p^{r-2}(p-1)\phi(p-1)$$

generators. □

Power Residues. Let p, as above, be an odd prime.

DEFINITION 122. An **n^{th} power residue mod p** is any $a \in (\mathbb{Z}/p\mathbb{Z})^*$ that can be written as an n^{th} power mod p. (For $n = 2$, this is called a **quadratic residue**; if $n = 3$ a cubic residue, and so on.)

THEOREM 123. *$a \in (\mathbb{Z}/p\mathbb{Z})^*$ is an n^{th} power residue $\iff$ $a^{\frac{p-1}{(n,p-1)}} \underset{(p)}{\equiv} 1$. (In this case, $x^n \underset{(p)}{\equiv} a$ has $(n, p-1)$ solutions.)*

PROOF. Use the isomorphism

$$\begin{array}{ccc} ((\mathbb{Z}/p\mathbb{Z})^*, \cdot) & \xrightarrow{\cong} & (\mathbb{Z}/(p-1)\mathbb{Z}, +), \\ m & \longmapsto & g^m \end{array}$$

where g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. We have $a = g^m$ for some m, so

$$\begin{aligned} a \underset{(p)}{\equiv} x^n \text{ for some } x(=g^y, \text{say}) &\iff m \underset{(p-1)}{\equiv} ny \text{ for some } y \in \mathbb{Z}/(p-1)\mathbb{Z} \\ &\iff (n, p-1) \mid m \text{ (by Theorem II.B.5(i))} \\ &\iff (p-1) \mid m \cdot \tfrac{p-1}{(n,p-1)} \\ &\iff a^{\frac{p-1}{(n,p-1)}} (= g^{m \cdot \frac{p-1}{(n,p-1)}}) \underset{(p)}{\equiv} 1. \end{aligned}$$

The number of solutions comes directly from Theorem II.B.5(ii). □

Since $(p-1, 2) = 2$, we have the

COROLLARY 124 (Euler's criterion). *$a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a quadratic residue $\iff a^{\frac{p-1}{2}} \underset{(p)}{\equiv} 1$.*[4]

We will use this in our discussion of quadratic reciprocity.

By Theorem 123, every n^{th} power residue, i.e. each element in the image of

$$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{(\cdot)^n} (\mathbb{Z}/p\mathbb{Z})^*$$

has preimage consisting of $(n, p-1)$ elements. So the map is $(n, p-1) : 1$, and the image contains $\frac{p-1}{(n,p-1)}$ elements.

COROLLARY 125. *Exactly $\frac{p-1}{(n,p-1)}$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are n^{th} power residues.*

EXAMPLE 126. $(\mathbb{Z}/7\mathbb{Z})^*$ has

- $3 = \frac{6}{(2,6)}$ quadratic residues: 1, 2, and 4. (By Euler, these must cube to 1.)
- $2 = \frac{6}{(3,6)}$ cubic residues: 1 and 6. (By Theorem 123, these must square to 1.)

[4]The only other possibility is to have $a^{\frac{p-1}{2}} \underset{(p)}{\equiv} -1$.

- $3 = \frac{6}{(4,6)}$ quartic residues: same as quadratic.
- $6 = \frac{6}{(5,6)}$ quintic residues: everything.

Quadratic reciprocity. We conclude our discussion of congruences with a famous and powerful result of Gauss that aids in determining when one prime is a quadratic residue modulo another. Write QR for "quadratic residue" and NR for "quadratic non-residue".

Recall that for an odd prime p, and integer a coprime to p, we have **Euler's criterion** (Corollary 124):

$$a \text{ is a QR mod } p \iff a^{\frac{p-1}{2}} \underset{(p)}{\equiv} 1.$$

Notice that in fact

$$(\mathbb{Z}/p\mathbb{Z})^* \xrightarrow{(\cdot)^{\frac{p-1}{2}}} \{+1, -1\} \cong \mathbb{Z}/2\mathbb{Z} \tag{22}$$

is a group homomorphism, which implies the

COROLLARY 127. *QR* $\times$ *QR* $=$ *QR, QR* $\times$ *NR* $=$ *NR, and NR* $\times$ *NR* $=$ *QR.*

You'll also recall that $x^2 \underset{(p)}{\equiv} -1$ is solvable if and only if $p \underset{(4)}{\equiv} 1$ (for p an odd prime; cf. Cor. II.B.9). We get a very quick re-proof of that result by Euler's criterion:

COROLLARY 128. -1 *is a QR mod* $p \iff p \underset{(4)}{\equiv} 1$ ($\underset{\text{Thm. II.B.10}}{\iff}$ p *splits in* $\mathbb{Q}(\sqrt{-1})$).

PROOF. $\frac{p-1}{2}$ is even iff $p \underset{(4)}{\equiv} 1$. Apply Euler. □

DEFINITION 129. For p an odd prime, the **Legendre symbol** is

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a QR mod } p, \\ -1 & \text{if } a \text{ is a NR mod } p. \end{cases}$$

Some easy properties of the symbol are:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ [by Cor. 127]

- $\left(\frac{a+pk}{p}\right) = \left(\frac{a}{p}\right)$
- $\left(\frac{a^2}{p}\right) = 1$ if $(p, a) = 1$.

EXAMPLE 130. $\left(\frac{6}{101}\right) = \left(\frac{3^2 \cdot 6}{101}\right) = \left(\frac{54}{101}\right) = \left(\frac{54+2\cdot 101}{101}\right) = \left(\frac{256}{101}\right) = \left(\frac{(16)^2}{101}\right) = 1$.

LEMMA 131 (Gauss). *Let p be an odd prime, $(a, p) = 1$. Consider the set $\mathcal{S} := \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$, and reduce it modulo p to a subset $\bar{\mathcal{S}}$ of $\{\frac{-p+1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$. Denote by ν the number of negative integers in this subset; then*

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

PROOF. Since there is no pair of elements of $\mathcal{S}$ with sum divisible by p, no pair of the form $\{b, -b\}$ can belong to $\bar{\mathcal{S}}$. As $\mathcal{S}$ (hence $\bar{\mathcal{S}}$) consists of $\frac{p-1}{2}$ distinct elements, $\bar{\mathcal{S}}$ contains either 1 or -1, either 2 or -2, and so on up to $\pm\frac{p-1}{2}$. Accordingly, write

$$\bar{\mathcal{S}} = \{\epsilon_1 \cdot 1, \epsilon_2 \cdot 2, \ldots, \epsilon_{\frac{p-1}{2}} \cdot \tfrac{p-1}{2}\}$$

where each ϵ_i is $+1$ or -1.

Multiplying all the elements of $\mathcal{S}$ together, and using the fact that "$\mathcal{S} \underset{(p)}{\equiv} \bar{\mathcal{S}}$", we have

$$(1a)(2a)\cdots(\tfrac{p-1}{2}a) \underset{(p)}{\equiv} (\epsilon_1 \cdot 1)(\epsilon_2 \cdot 2)\cdots(\epsilon_{\frac{p-1}{2}}\tfrac{p-1}{2})$$

which after cancellations becomes

$$a^{\frac{p-1}{2}} \underset{(p)}{\equiv} \epsilon_1\epsilon_2\cdots\epsilon_{\frac{p-1}{2}} = (-1)^{\nu},$$

which by Euler's criterion is $\left(\frac{a}{p}\right)$. □

EXAMPLE 132 ($p = 11$, $a = 3$). $\mathcal{S} = \{3, 6, 9, 12, 15\}$, and $\bar{\mathcal{S}} = \{3, -5, -2, 1, 4\}$ has two negative numbers; so $\left(\frac{3}{11}\right) = (-1)^2 = 1$ and 3 is a QR mod 11 (indeed $3 \underset{(11)}{\equiv} 5^2$).

LEMMA 133. *Let p be an odd prime, $a > 0$ with $(a, p) = 1$. Then $\left(\frac{a}{p}\right)$ depends only on p modulo $4a$: for prime $q \underset{(4a)}{\equiv} \pm p$, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

We will defer the proof to after that of the following main

THEOREM 134 (Quadratic Reciprocity Law). *Let p and q be distinct odd primes. Then*

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

More concretely, this result (which we'll abbreviate QRL) says that

- $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if $p \underset{(4)}{\equiv} 1$ or $q \underset{(4)}{\equiv} 1$

and

- $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \underset{(4)}{\equiv} 3 \underset{(4)}{\equiv} q$.

PROOF OF QRL. Consider first the case $p \underset{(4)}{\equiv} q$. We may assume $p > q$, so that $p = q + 4a$, $a > 0$. Then

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{2^2}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right),$$

while

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right) = \left(\frac{-4a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2^2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)$$

which by Lemma 133 is $(-1)^{\frac{p-1}{2}}\left(\frac{a}{q}\right)$. So the result follows in this case.

Now suppose $p \underset{(4)}{\not\equiv} q$. Then $p \underset{(4)}{\equiv} -q$, and so $p = -q + 4a$, $a > 0$, and

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{-p+4a}{p}\right) = \left(\frac{q}{p}\right)$$

where we used Lemma 133 in the middle equality. □

REMARK 135. How to deal with the prime 2? One has the following complement to the QRL:[5]

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}} = \begin{cases} +1 & \text{if } p \underset{(8)}{\equiv} \pm 1 \\ -1 & \text{if } p \underset{(8)}{\equiv} \pm 3. \end{cases}$$

EXAMPLE 136. Since $5 \underset{(4)}{\equiv} 1$, QRL $\implies \left(\frac{5}{103}\right) = \left(\frac{103}{5}\right) = \left(\frac{3}{5}\right) = -1$. So $x^2 \underset{(103)}{\equiv} 5$ has no solutions.[6]

Similarly, since $101 \underset{(4)}{\equiv} 1$, QRL $\implies \left(\frac{101}{613}\right) = \left(\frac{613}{101}\right) = \left(\frac{7}{101}\right) = \left(\frac{101}{7}\right) = \left(\frac{3}{7}\right) = -1$.

We now turn to the

PROOF OF LEMMA 133. As above write $\mathcal{S} = \{a, 2a, \ldots, \frac{p-1}{2}a\}$. Put

$$I = \left(\tfrac{p}{2}, p\right) \cup \left(\tfrac{3}{2}p, 2p\right) \cup \cdots \cup \left((b - \tfrac{1}{2})p, bp\right)$$

where $b = \lfloor \frac{a}{2} \rfloor$. I claim that *every element of* $\mathcal{S}$ *which is* $\underset{(p)}{\equiv}$ *to something in* $\left(-\frac{p}{2}, 0\right)$, *lies in* I.

First consider the case $b = \frac{a}{2}$. We have $bp = \frac{a}{2}p > \frac{p-1}{2}a$, so the Claim is OK here. The other case is where $b = \frac{a-1}{2}$: from $bp + \frac{p}{2} = \frac{a-1}{2}p + \frac{p}{2} = \frac{pa}{2} > \frac{p-1}{2}a$, it follows that $\left((b - \frac{1}{2})p, bp\right)$ is the last interval that could contain an element of $\mathcal{S}$ that reduces to $\left(-\frac{p}{2}, 0\right)$. Claim is proved.

With ν as in Lemma 131 and its proof, we have $\left(\frac{a}{p}\right) = (-1)^\nu$ which by our Claim $= (-1)^{|\mathcal{S} \cap I|}$. Now writing $\frac{1}{a}\mathcal{S} = \{1, 2, 3, \ldots, \frac{p-1}{2}\}$ and

$$\frac{1}{a}I = \left(\tfrac{p}{2a}, \tfrac{p}{a}\right) \cup \left(\tfrac{3p}{2a}, \tfrac{2p}{a}\right) \cup \cdots \cup \left(\tfrac{2b-1}{2a}p, \tfrac{bp}{a}\right) \subset \left(0, \tfrac{p}{2}\right),$$

we find

$$|\mathcal{S} \cap I| = |\tfrac{1}{a}\mathcal{S} \cap \tfrac{1}{a}I| = |\mathbb{Z} \cap \tfrac{1}{a}I|.$$

[5]A proof may be found in [NZM] §3.3.

[6]Or, if you prefer not to use QRL, you can just compute 5^{51} mod 103. Good luck with that.

By the division algorithm, we can write $p = 4ac + r$, and note that

$$J := \left(\tfrac{r}{2a}, \tfrac{r}{a}\right) \cup \left(\tfrac{3r}{2a}, \tfrac{2r}{a}\right) \cup \cdots \cup \left(\tfrac{2b-1}{2a}r, \tfrac{br}{a}\right)$$

is just $\frac{1}{a}I$ with endpoints of intervals moved by even integers. So

$$(\nu =) \left|\mathbb{Z} \cap \tfrac{1}{a}I\right| \underset{(2)}{\equiv} |\mathbb{Z} \cap J|,$$

which already proves that $\left(\frac{a}{p}\right)$ dependson p only modulo $4a$.

We only need to check now that if $q \underset{(4a)}{\equiv} -p$, we get the same result. In the above computation, this means replacing r by $4a - r$, hence J by

$$\left(2 - \tfrac{r}{2a}, 4 - \tfrac{r}{a}\right) \cup \left(6 - \tfrac{3r}{2a}, 8 - \tfrac{2r}{a}\right) \cup \cdots \cup \left(4b - 2 - \tfrac{2b-1}{2a}r, 4b - \tfrac{br}{a}\right),$$

which is $-J$ with endpoints moved by even integers. I rest my case. □

There is a generalization of the Legendre symbol to (some) composite moduli.

DEFINITION 137. Let n be a positive odd integer, with prime factorization $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. The **Jacobi symbol** is given by

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}$$

(or by 1, if $n = 1$).

The three easy properties of the Legendre symbol, and the QRL, carry over *verbatim*. (For instance, $\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{\frac{n-1}{2}\frac{a-1}{2}}$ as long as n and a are odd and coprime.) The main difference is that $\left(\frac{a}{n}\right) = 1$ does *not* imply that a is a QR mod n. This is because, by the Chinese Remainder Theorem,

$$a = \text{QR mod } n \underset{\text{CRT}}{\iff} a = \text{QR mod each } p_i^{\alpha_i}$$

$$\underset{\text{Hensel}}{\iff} a = \text{QR mod each } p_i \iff \left(\frac{a}{p_i}\right) = 1 \ (\forall i),$$

while (on the other hand)

$$\left(\frac{a}{n}\right) = 1 \iff \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i} = 1$$

is much weaker.

The Jacobi symbol also leads to a *new primality test*: given $(a, n) = 1$, calculate $\left(\frac{a}{n}\right)$ and $a^{\frac{n-1}{2}} \pmod{n}$. If they differ, obviously n is composite. But wait: how do you compute $\left(\frac{a}{n}\right)$ without knowing $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$? *By using the QRL!!* Flip it, after reducing a mod n of course; applying this repeatedy is very similar to the Euclidean Algorithm for computing the GCD! Computationally, this is the true importance of quadratic reciprocity.

Exercises

(1) Use Hensel's Lemma to solve $x^3 + x + 57 \underset{(5^3)}{\equiv} 0$.

(2) Use quadratic reciprocity to compute the Legendre symbol $\left(\frac{41}{97}\right)$. Then state your result in terms of solubility or insolubility of a congruence.

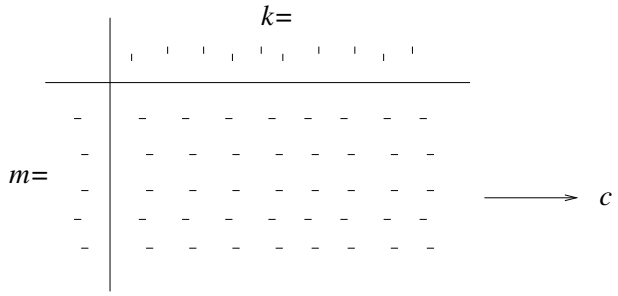
Part 3

Introduction to cryptography

CHAPTER 12

Symmetric ciphers

Suppose two parties want to exchange a sensitive message. Let's call them **S**ender and **R**eceiver. They have an agreed-upon key k, and a big lookup-table[1] **M**:



You plug in the key k and message m, and look up the encoded message c. We can also write this a bit more formally, as a map of sets:

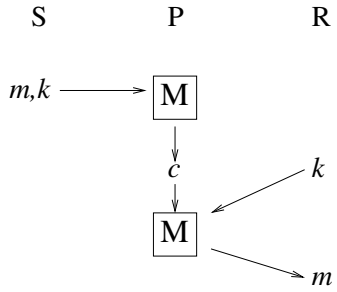
$$\mathbf{M}: \ \mathcal{K} \times \mathcal{M} \to \mathcal{C},$$

where $\mathcal{K}$ denotes the set of possible keys, $\mathcal{M}$ the set of possible messages ("plaintext"), and $\mathcal{C}$ the set of possible ciphertexts. To decode, you look up the column under k, find c, and deduce m. (Obviously the entries of each column all need to be distinct.) We'll write this as

$$c = \mathrm{M}_k(m) \ , \ \ m = \mathrm{M}_k^{-1}(c).$$

[1] **M** need not *literally* be a table; more likely, it's a function. But this is really the same thing.

Here is the whole process in a schematic picture:



where P(=Public) means that c is visible to everyone, including a would-be interceptor **I**. For this to work successfully, **M** must be *easy* to use forward and in reverse (given any k). Moreover, it should be reasonably secure:[2]

- Given one or more ciphertexts

  $$c_i = \mathrm{M}_k(m_i)\ ,\ \ i = 1, \ldots, n$$

  encrypted using the key k, it should be *hard* to compute any of the m_i without knowing k, let alone to deduce k.
- Given one or more ciphertext/plaintext pairs, viz.

  $$(m_1, c_1), \ldots, (m_n, c_n),$$

  it should be hard to deduce k or determine any other m from $c = \mathrm{M}_k(m)$. ("chosen plantext attack")

Most of the "obvious" ideas don't achieve these security objectives:

- simple substitution ciphers — monoalphabetic, hence easy to break by frequency analysis (i.e. by considering the most-used letters and letter-pairs), cf. [HPS] pp. 1-10.
- polyalphabetic ciphers (e.g. Vigenère) — uses keyword k to (cyclically) prescribe how to shift each letter in m, cf. [HPS] p. 198. Not vulnerable to naive frequency analysis, but repeated fragments *can* allow the key length to be guessed, andthen there are statistical methods to recover the keyword.

[2]Kerchoff's principle: you have to assume that **I** knows the encryption scheme **M**.

The remaining methods presume that the message has been numerically encoded using (say) ASCII, which turns each letter into a byte (= 8 bits), e.g.

$$\begin{array}{cccccccc} & & & & \underline{\text{binary}} & & \underline{\text{hexadecimal}} \\ A & \to & 65 & \underset{\text{base 2}}{\to} & \underbrace{0100}\underbrace{0001} & \longleftrightarrow & 41 \\ Z & \to & 90 & \to & \underbrace{0101}\underbrace{1010} & \longleftrightarrow & 5a \end{array}$$

- binary XOR — m, k = binary numbers; perform bitwise addition "$m \oplus k$": e.g. if $k = 11001100\,(= cc)$, we send $A \mapsto 10001101\,(= 8d)$, $Z \mapsto 10010110\,(= 96)$. Doing $\oplus k$ again inverts it. Obviously it's alright to use k once (for one m), but
$$(\underbrace{m_1 \oplus k}_{c_1}) \oplus (\underbrace{m_2 \oplus k}_{c_2}) = m_1 \oplus m_2$$
should make you nervous about even using it twice! Moreover, if **I** knows (m_1, c_1) then s/he knows $k = m_1 \oplus (m_1 \oplus k) = m_1 \oplus c_1$.
- multiplication mod p — $m \in \mathbb{Z}_p$, $k \in \mathbb{Z}_p^* \longmapsto c := k \cdot m \pmod p$. Of course, this is easy to invert: use the Euclidean algorithm to find $k^{-1} \pmod p$. Unfortunately, it's easy to break: if **I** knows (m, c) then s/he knows $k = m^{-1} \cdot c \pmod p$ unless $m = 0$.
- One can also consider shift ($m \mapsto m + k \bmod p$) modulo p and affine ($m \mapsto k_1 \cdot m + k_2 \bmod p$) c ciphers. These have the same problems.

Slightly trickier is to work in a finite field of *prime power* order such as $\mathbb{F}_{2^8}$, which may be thought of as the set of polynomials of degree ≤ 7 with binary (i.e. $\mathbb{Z}_2$) coefficients, with addition and multiplication modulo the polynomial $x^8 + x^4 + x^3 + x + 1$. But this is breakable too.

So what *does* work? We don't want to have to use (hence transmit . . . beforehand? how?) keys as long as our message, choosing a new key for every message — this is no better than meeting in secret

to exchange the message! Here's one idea: a *pseudorandom number generator*, that is, a function

$$\mathcal{R} : \mathcal{K} \times \mathbb{N} \to \mathbb{Z}_2 \, (= \{0,1\})$$

satisfying

(1) $\mathcal{R}$ is *easy* to compute
(2) k is *hard* to determine from $\underbrace{\mathcal{R}(k,1),\, \mathcal{R}(k,2) \ldots, \mathcal{R}(k,n)}_{(*)}$, say
(3) $\mathcal{R}(k,n+1), \mathcal{R}(k,n+2), \ldots$ are *hard* to determine from $(*)$.

Then you can start with a (relatively) short k, generate the number

$$\mathcal{R}(k,1)\mathcal{R}(k,2) \cdot \cdots \cdot \mathcal{R}(k,n)$$

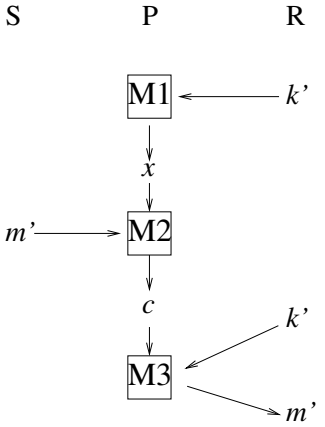
and XOR this with a binary message (of length N). While one doesn't know if (in a rigorous mathematical sense) pseudorandom number generators *exist*, this is part of the idea behind the AES (Advanced Encryption Standard) encryption scheme now widely used.

- AES encryption combines
  (a) shift operations,
  (b) pseudorandom number generator + XOR,
  (c) operations in $\mathbb{F}_{2^8}$, and
  (d) other messy mixing operations,
  all repeated about 10 times, and applies to a message (or message block) consisting of a 4×4 matrix of bytes (hence 128 bits).[3]

One question which arises in this discussion is the meaning of "hard" and "easy". Roughly, these are supposed to refer to applications that require exponential resp. polynomial time in the bit-length. Especially when we discuss public key stuff and related mathematical problems, it becomes clear that this is intimately related to the $1,000,000 "P vs. NP" problem. So to a certain extent the whole subject is currently running on "faith and experience"!

[3]See pp. 33-34 of the AES document I have linked to on the webpage. AES takes (k,m) as input and outputs c (or (k,c) as input and outputs m).

Another key question that comes up is, how do the parties *share* the key k in advance? The key need not be as long as the message, so this is our opportunity to use something slower but ingenious and very secure. All three of these terms describe the various public key cryptography (or "asymmetric cipher") systems, the idea of which (in a picture) is:



The setup is asymmetric because **S** does not (need to) know k; s/he only uses x to encode m. **R** alone knows k, and **R** alone should be able to "read" c.

The tricky point here is that the *message* m' then could *become* the key k in something like AES. That is, **S** and **R** use a public key system — an (inefficient) asymmetric cipher — to share a key, which is then used in a symmetric cipher system to transmit efficiently a long message m.

REMARK. There is a supplementary reading assignment attached to this section: read pp. 1-10, 37-47, and 59-62 in [HPS].

The links posted on the webpage beside the link to these notes (on Public Key Cryptography, AES encoding, and computational complexity) are optional.

Exercises

(1) Convert the decimal numbers 8734 and 5177 into binary numbers, combine them using XOR, then convert back to decimal.

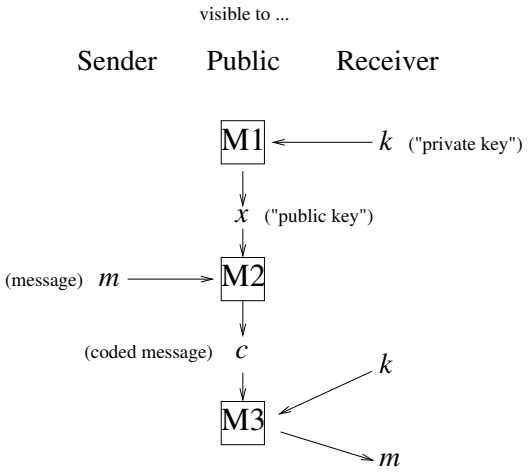
(You could think of 8734 as amessage to be encrypted and 5177 as the key.)

(2) Decrypt one of the messages in Hoffstein-Pipher-Silverman problem 1.4 (p. 48, a, b, or c – your choice).

CHAPTER 13

Public key cryptography

Consider once more the "asymmetric cipher" diagram (with a slight notational reset):



We recall that the meaning of "Public" is that x and c are transmitted over an insecure channel, and thus visible to anyone. Roughly speaking, M2 is a function (partly determined by x) from $\mathcal{M}$ to $\mathcal{C}$ which is *easy* to compute but *hard* to invert . . . without knowledge of k, which once again makes it easy.[1]

For this picture to be feasible, then, we must have such a "**trapdoor function**". This is based upon the widely held belief that P $\neq$ NP; that is, that there are mathematical problems *not* solvable in polynomial time, even though a solution *can* be *verified* in polynomial time.[2] A special case is the idea of a function whose inverse is hard to compute, even though computing the function (and hence verifying a value of the inverse) goes quickly.

[1] In the above, *M3 together with k* provides an inverse for *M2 together with x*.

[2] I have posted links to further discussion of the P vs. NP problem.

EXAMPLE 138. It is considered easier to . . .

(a) verify a prime factorization than to factor a number

(b) compute powers mod N (e.g. by fast-powering) than to compute "logarithms" mod N

(c) compute powers mod N than to compute roots mod N (if N is composite with unknown factors).

Here (b) leads to the Diffie-Hellman key exchange and the El Gamal cryptosystem, while (a) and (c) lead to the RSA cryptosystem.

What is a logarithm modulo N?

DEFINITION 139. Take a prime p, and an integer a with $(a, p) = 1$. If $s \underset{(p)}{\equiv} a^m$ for some m, then m is the **discrete logarithm** of s (mod p) to the base a (sometimes written $\log_a s$).

If $a = g$ is a generator, then any s coprime to p can be written as g^m. The **DLP** (**discrete log problem**) is the problem of computing $m = \log_g a$. Notice that this is precisely the problem of computing the inverse of the isomorphism

$$\begin{array}{ccc} \mathbb{Z}/(p-1)\mathbb{Z} & \overset{\cong}{\to} & (\mathbb{Z}/p\mathbb{Z})^*. \\ m & \mapsto & g^m \end{array}$$

Also note that, like the usual log, $g^{m+n} = \underbrace{g^m}_{\alpha}\underbrace{g^n}_{\beta} \underset{\log_g}{\Longrightarrow} \log_g(\alpha\beta) = m + n = \log_g(\alpha) + \log_g(\beta)$.

Here is how to use this to arrive at a shared secret (but not yet a *cryptosystem* of the form in the diagram). Since the relationship is symmetric here, we'll replace **S**(ender) and **R**(eceiver) by **A** and **B**, who openly agree on a pair (p, g) where p is a prime and g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ (i.e. a primitive root mod p). Then **A** and **B** each choose (random) numbers $\alpha, \beta \in \mathbb{Z}/(p-1)\mathbb{Z}$ and send each other $g^\alpha, g^\beta \in (\mathbb{Z}/p\mathbb{Z})^*$. The shared secret is then this:

$$\left.\begin{array}{l} \textbf{A} \text{ computes } (g^\beta)^\alpha = g^{\alpha\beta} \\ \textbf{B} \text{ computes } (g^\alpha)^\beta = g^{\alpha\beta} \end{array}\right\} =: s.$$

The eavesdropper **E** sees p, g, g^α, and g^β. In order to find $g^{\alpha\beta}$, s/he *would have to compute* $\log(g^\alpha)$ (or $\log(g^\beta)$) to find α (or β); then s/he can just do $(g^\beta)^\alpha$. But the first step here is the DLP, and if p has say 200 digits this is an impossible step!

EXAMPLE 140 ($p = 11$). Repeatedly mulitplying by 2

$$1 \xrightarrow{\cdot 2} 2 \xrightarrow{\cdot 2} 4 \xrightarrow{\cdot 2} 8 \xrightarrow{\cdot 2} 5 \xrightarrow{\cdot 2} 10 \xrightarrow{\cdot 2} 9 \xrightarrow{\cdot 2} 7 \xrightarrow{\cdot 2} 3 \xrightarrow{\cdot 2} 6 \xrightarrow{\cdot 2} 1$$

shows that $g = 2$ is a generator (how many more are there?). Now Alice chooses $\alpha = 6$ and sends

$$g^\alpha = 2^6 = 64 \underset{(11)}{\equiv} 9 \text{ to Bob,}$$

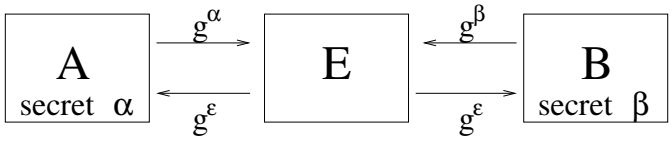
while Bob chooses $\beta = 7$ and sends

$$g^\beta = 2^7 = 128 \underset{(11)}{\equiv} 7 \text{ to Alice.}$$

Bob then computes $9^\beta = 9^7 \underset{(11)}{\equiv} (-2)^7 = (-2)(-2)^2(-2)^{2^2} \underset{(11)}{\equiv} (-2)\cdot 4 \cdot 5 \underset{(11)}{\equiv} 4$ while Alice computes $7^\alpha = 7^6 = 343^2 \underset{(11)}{\equiv} 2^2 = 4$. Both obtain $s = 4$.

Notice that **A** and **B** can't decide what s will be beforehand (without solving the DLP themselves), so this isn't a means of transmitting messages, only of arriving at a shared secret key s. It is known as the **Diffie-Hellman key exchange**.

Let's look briefly at one possible security issue, the "(wo)man-in-the-middle attack". Remember p and g are public.



Here **E** has intercepted (and "confiscated") **A**'s and **B**'s communications to each other, and sent them both her own g^ε (with $\varepsilon =$ *her* secret). Now **A** will compute $(g^\varepsilon)^\alpha = g^{\alpha\varepsilon}$ and **B** will compute $(g^\varepsilon)^\beta = g^{\beta\varepsilon}$. They unwittingly use these numbers as a symmetric cipher (e.g. in AES) to transmit a confidential message. Since **E** can

compute $(g^\alpha)^\varepsilon = g^{\alpha\varepsilon}$ and $(g^\beta)^\varepsilon = g^{\beta\varepsilon}$, she can read both of their messages, and then re-encrypt then using $g^{\beta\varepsilon}$ resp. $g^{\alpha\varepsilon}$ to send them on to the other party. Neither **A** nor **B** is aware of the breach in security!

Exercises

(1) Agnes and Bert use Diffie-Hellman key exchange to produce a shared secret key. They agree on $p = 101$ and an element $g = 15$ of order $p - 1$, both of which have been made public. Agnes chooses α and sends $g^\alpha = 42 \pmod{101}$ to Bert, while Bert has chosen β and sent $g^\beta = 24$ to Agnes. As Ivan the interceptor, you overhear all this. By checking the first few powers of g mod 101, try to produce α or β and hence their secret key s.

(2) Note that $2^3 \underset{(23)}{\equiv} 8$. By finding an inverse of 3 in $\mathbb{Z}/22\mathbb{Z}$, find an integer x such that $8^x \underset{(23)}{\equiv} 2$.

(3) Compute the following discrete logarithms: (a) $\log_2 13$ in $\mathbb{Z}/23\mathbb{Z}$, and $\log_{10}(22)$ in $\mathbb{Z}/47\mathbb{Z}$.

CHAPTER 14

Discrete log problem

In the last section, we described how the difficulty of computing discrete logarithms (the power to which a generator $g \in (\mathbb{Z}/p\mathbb{Z})^*$ must be raised to obtain a given $a \in (\mathbb{Z}/p\mathbb{Z})^*$) allows two correspondents to share a (random) secret key over an insecure channel (Diffie-Hellman). What we shall now explain is how to turn this into a *bona fide* cryptosystem that can be used to exchange *messages* (or a *non*-random secret key). I'll use as before **S** for Sender, **R** for Receiver, and **E** for Eavesdropper.

El Gamal cryptosystem. There are four steps:

- **S** and **R** openly agree on a prime modulus p and generator $g \in (\mathbb{Z}/p\mathbb{Z})^*$.
- **R** chooses a *private key* $\rho \in \mathbb{Z} \cap [1, p-2]$, computes the *public key* $r = g^\rho$, and sends this to **S**.
- **S** chooses an *ephemeral key* $\sigma \in \mathbb{Z} \cap [1, p-2]$, a *plaintext message* $m \in \mathbb{Z}/p\mathbb{Z}$, and sends **R** the *ciphertext* $(c_1, c_2) := (g^\sigma, mr^\sigma)$ (both mod p); σ is then discarded.
- **R** decrypts the ciphertext by computing

$$c_1^{-\rho} \cdot c_2 \underset{(p)}{\equiv} g^{-\sigma\rho} \cdot mg^{\sigma\rho} \underset{(p)}{\equiv} m.$$

That's it.

Now, **E** overhears p, g, r, and (c_1, c_2). If σ were used to encode a *second* message m' as (c_1', c_2'), then s/he could compute

$$\frac{c_2'}{c_2} = \frac{m'r^\sigma}{mr^\sigma} = \frac{m'}{m}.$$

Otherwise, it seems difficult to discover the message: in fact, *an algorithm for cracking El Gamal could also be used to crack Diffie-Hellman*.

Indeed, in Diffie-Hellman, **A** and **B** send each other g^α and g^β (mod p). **E** then enters (as data for the algorithm breaking El Gamal) p, g, g^α, and (g^β, c_2), with c_2 arbitrary. The algorithm computes

$$(g^\beta)^{-\alpha} \cdot c_2 = g^{-\alpha\beta} c_2,$$

and then **E** can divide out c_2 and invert the result to get $g^{\alpha\beta}$. So in this sense, El Gamal is probably secure.

Discrete log problem (DLP) revisited. Of course, it is also true that El Gamal and Diffie-Hellman are no more secure than the DLP is hard. To describe "how hard", we'll introduce some notation:

DEFINITION 141. Let $f, g > 0$ be functions of x.
(i) $f(x) = \mathcal{O}(g(x)) \iff \exists\, c, C \geq 0$ s.t. $f(x) \leq cg(x)\ \forall x \geq C$.
(ii) $f(x) = \Omega(g(x)) \iff \exists\, \tilde{c}, \tilde{C} \geq 0$ s.t. $f(x) \geq \tilde{c}g(x)\ \forall x \geq C$.
(iii) $f(x) = \Theta(g(x)) \iff f = \mathcal{O}(g)$ *and* $\Omega(g)$.
(iv) $f(x)$ grows **exponentially** $\iff \exists\, \alpha, \beta > 0$ s.t. $\Omega(x^\alpha) = f(x) = \mathcal{O}(x^\beta)$.
(v) $f(x)$ grows **polynomially** $\iff \exists\, \alpha, \beta > 0$ s.t. $\Omega((\log x)^\alpha) = f(x) = \mathcal{O}((\log x)^\beta)$.
(vi) $f(x)$ grows **sub-exponentially** $\iff \forall\, \alpha, \beta > 0\ \Omega((\log x)^\alpha) = f(x) = \mathcal{O}(x^\beta)$.

Here, "polynomial", "exponential", etc. mean *in the bitlength* $\log_2 x$. Note that (since $\frac{f(x)}{g(x)} < L + 1$ for $x \geq C$ gives $f(x) < (L+1)g(x)$ for $x \geq C$) we have

$$L := \lim_{x\to\infty} \frac{f(x)}{g(x)} \text{ finite } \implies f(x) = \mathcal{O}(g(x)),$$

but *not* conversely: take $f(x) = \cos(x)$, $g(x) = 1$; then L doesn't exist, but $f(x) = \mathcal{O}(g(x))$.

REMARK 142. (a) A brute-force approach to the DLP: we want to solve $g^x \underset{(p)}{\equiv} a$, where g is a generator[1] and a is arbitrary. List

[1]Slightly more generally, one could take g to be an element of order N in $(\mathbb{Z}/p\mathbb{Z})^*$, and $a \in \langle g \rangle$. Then the running time is $\mathcal{O}(N)$.

$1, g, g^2, \ldots, g^{p-2}$; a must appear. This requires exponential time — more precisely, $\mathcal{O}(p)$.

(b) There is a faster (but still exponential-time) approach we describe next; while the *index calculus* gives a sub-exponential-time algorithm for DLP.[2]

(c) The "elliptic curve discrete log" -based cryptosystems we'll encounter later in this course appear to be more secure, because only exponential time algorithms exist for elliptic DLP.

(d) The "additive discrete log" problem is that of solving $b \cdot x \underset{(p)}{\equiv} a$. Obviously this can be solved in polynomial time (using the Euclidean algorithm), and we don't base any cryptosystems on that.

Babystep-Giantstep. This is the nickname for an algorithm due to Shanks. Let $g \in (\mathbb{Z}/p\mathbb{Z})^*$ be a generator;[3] we want to solve $g^x \underset{(p)}{\equiv} a$.

- Let $n = 1 + \lfloor \sqrt{p} \rfloor$.
- Make 2 lists: $1, g, g^2, \ldots, g^n$ (babystep); $a, a \cdot g^{-n}, a \cdot g^{-2n}, \ldots, a \cdot g^{-n^2}$ (giantstep).
- Find a match, say

$$g^i = a \cdot g^{-jn} \tag{23}$$

  between the two lists.
- Put $x = i + jn$.

This gives a solution, since $g^x = g^i \cdot g^{jn} = a$ by (23).

REMARK 143. (a) *Why is there always a match?* There must be a solution $x = nq + r$ ($0 \le r < n$), and then (using $n > \sqrt{p}$)

$$q = \frac{x - r}{n} < \frac{p}{n} < \sqrt{p} < n,$$

so that $g^x \underset{(p)}{\equiv} a$ becomes $g^r \underset{(p)}{\equiv} a \cdot g^{-qn}$ (with $0 \le r < n$, $0 \le q < n$).

(b) *What is the running time?* Making the lists requires $2n$ multiplications, hence is $\mathcal{O}(\sqrt{p}(\log p)^c)$ (where the logarithmic factor

[2] See §3.8 of [HPS].

[3] again, more generally we could instead take an element of order N

reflects the time to perform multiplications). The matching step is $\mathcal{O}(\log p)$ so doesn't change this. While this is an improvement over $\mathcal{O}(p)$ it is still exponential time.

EXAMPLE 144 ($p = 97$, $g = 5$, $a = 80$). We solve $5^x = 80$:
- $n = 1 + \lfloor \sqrt{97} \rfloor = 10$.
- list 1 : $1, \boxed{5}, 25, 28, 43, 21, 8, 40, 6, 30, 53$ (mult. by 5)
- list 2 : $80, 7, 77, 71, \boxed{5}, \ldots$ (mult. by $5^{-10} \underset{(p)}{\equiv} 53^{-1} \underset{(p)}{\equiv} 11$)
- The match is $g^1 \underset{(p)}{\equiv} a \cdot g^{-4\cdot 10} (\underset{(p)}{\equiv} 5)$.
- $x = 1 + 4 \cdot 10 = 41$.

Pohlig-Hellman Algorithm. If you know the Chinese Remainder Theorem, there is a massive potential simplification staring you in the face:

$$97 - 1 = 96 = 2^5 \cdot 3$$

$\Longrightarrow$

$$\begin{array}{ccccc} (\mathbb{Z}/97\mathbb{Z})^* & \cong & \mathbb{Z}/96\mathbb{Z} & \underset{\text{CRT}}{\cong} & \mathbb{Z}/2^5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \\ g^x & \longleftrightarrow & x & \longleftrightarrow & (y, z) \end{array} \tag{24}$$

Now, two elements $\mu, \eta \in \mathbb{Z}/96\mathbb{Z}$ are equal if and only if $\mu \underset{(2^5)}{\equiv} \eta$ and $\mu \underset{(3)}{\equiv} \eta$, or equivalently, $3\mu \underset{(96)}{\equiv} 3\eta$ and $2^5\mu \underset{(96)}{\equiv} 2^5\eta$. On the left-hand side (multiplication) of (24), this says two elements $M, N \in (\mathbb{Z}/97\mathbb{Z})^*$ are equal iff $M^3 \underset{(p)}{\equiv} N^3$ and $M^{2^5} \underset{(p)}{\equiv} N^{2^5}$. So if we can find y and z such that

$$(g^3)^y \underset{(p)}{\equiv} a^3 \text{ and } (g^{2^5})^z \underset{(p)}{\equiv} a^{2^5},$$

and take x to correspond to (y, z) under CRT, then $x = y + 2^5 y' = z + 3z'$

$$\Longrightarrow \begin{cases} (g^x)^3 \underset{(p)}{\equiv} (g^3)^y (g^{96})^{y'} \underset{(p)}{\equiv} (g^3)^y \underset{(p)}{\equiv} a^3 \\ (g^x)^{2^5} \underset{(p)}{\equiv} (g^{2^5})^z (g^{96})^{z'} \underset{(p)}{\equiv} (g^{2^5})^z \underset{(p)}{\equiv} a^{2^5} \end{cases} \Longrightarrow g^x \underset{(p)}{\equiv} a.$$

The order of g^3 [resp. g^{2^5}] is 2^5 [resp. 3], so even the "brute-force" DLP running times will be "$\mathcal{O}(2^5)$" and "$\mathcal{O}(3)$".

EXAMPLE 145. $(g^{2^5})^z \underset{(p)}{\equiv} a^{2^5}$ is $35^z \underset{(97)}{\equiv} 61$. Powers of 35 are $35, 61, 1$, so $z = 2$.

This approach would be a mistake for the other congruence (as it would involve directly computing 2^5 powers of g^3). Instead, write

$$\gamma = g^3, \ \ \alpha = a^3, \text{ and } y = y_0 + 2y_1 + 2^2y_2 + 2^3y_3 + 2^4y_4.$$

To solve $\alpha \underset{(p)}{\equiv} \gamma^y$, note that γ has order 2^5 and compute

$$\alpha^{2^4} \underset{(p)}{\equiv} (\gamma^y)^{2^4} \underset{(p)}{\equiv} (\gamma^{2^4})^{y_0}$$

to get y_0,

$$\alpha^{2^3} \underset{(p)}{\equiv} (\gamma^y)^{2^3} \underset{(p)}{\equiv} (\gamma^{2^4})^{y_1} \cdot \gamma^{2^3 y_0}$$
$$\Longrightarrow \quad (\gamma^{2^4})^{y_1} \underset{(p)}{\equiv} (\alpha\gamma^{-y_0})^{2^3}$$

to get y_1, and so on, as we demonstrate below. At each step, the problem is a piece of cake because γ^{2^4} has order 2. (Other prime powers are dealt with in exactly the same way.)

EXAMPLE 146. We have $\gamma = g^3 \underset{(p)}{\equiv} 28$, $\gamma^{2^4} \underset{(p)}{\equiv} -1$ (because it has order 2), and $\alpha = a^3 \underset{(p)}{\equiv} 34$. Now compute:

$$(-1)^{y_0} \underset{(p)}{\equiv} \alpha^{2^4} \underset{(p)}{\equiv} -1 \quad \Longrightarrow \quad y_0 = 1;$$

$$(-1)^{y_1} \underset{(p)}{\equiv} (\alpha\gamma^{-y_0})^{2^3} \underset{(p)}{\equiv} (34 \cdot \underbrace{28^{-1}}_{52})^{2^3} \underset{(p)}{\equiv} (22)^{2^3} \underset{(p)}{\equiv} 1 \quad \Longrightarrow \quad y_1 = 0;$$

$$(-1)^{y_2} \underset{(p)}{\equiv} (\alpha\gamma^{-y_0-2y_1})^{2^2} \underset{(p)}{\equiv} (22)^{2^2} \underset{(p)}{\equiv} 1 \quad \Longrightarrow \quad y_2 = 0;$$

$$(-1)^{y_3} \underset{(p)}{\equiv} (\alpha\gamma^{-y_0-2y_1-2^2y_2})^2 \underset{(p)}{\equiv} 22^2 \underset{(p)}{\equiv} -1 \quad \Longrightarrow \quad y_3 = 1;$$

$$(-1)^{y_4} \underset{(p)}{\equiv} (\alpha\gamma^{-y_0-2y_1-2^2y_2-2^3y_3}) \underset{(p)}{\equiv} (34 \cdot \underbrace{28^{-9}}_{20}) \underset{(p)}{\equiv} 1 \quad \Longrightarrow \quad y_4 = 0$$

$\implies y = 9$. Combining this with $z = 2$, we have

$$x = 9 + 2^5 y' \underset{(3)}{\equiv} 2 \quad \implies \quad 2y' \underset{(3)}{\equiv} 2 \quad \implies \quad y' = 1$$

$\implies x = 9 + 32 = 41$.

The upshot of this algorithm[4] is that the DLP is easy when $p - 1$ is a product of small primes (essentially, $\mathcal{O}$ of $\{\text{the largest prime}\} \times \{\log p\}$). Hence, if one wants Diffie-Hellman or El Gamal to be secure, one must *avoid* such a choice of p.

Exercises

(1) Alice and Bob agree to use $(p, g) = (1373, 2)$ for ElGamal.
   (a) First, Alice will send a message to Bob. So he picks a private key $\rho_b = 716$ and computes the public key $r_b = 2^{716} \underset{(p)}{\equiv} 469$; Alice chooses an ephemeral key $\sigma_a = 877$ and message $m_a = 583$. What is the ciphertext that Alice sends to Bob?
   (b) Now they switch roles. Alice chooses a private key $\rho_a = 299$; what is her public key r_a? Bob encrypts a message using r_a and sends Alice the ciphertext $(c_1, c_2) = (661, 1325)$. Decrypt the message.
   (c) Finally, Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(c_1, c_2) = (693, 793)$ to Bob. You intercept the transmission. Decrypt the message by solving the appropriate discrete log problem.

(2) Show that (a) $5 + 6x^2 - 37x^5 = \mathcal{O}(x^5)$ and (b) $(\log k)^{375} = \mathcal{O}(k^{0.001})$.

(3) Use babystep-giantstep to solve the following discrete log problems. (Do the first one on paper. Try writing a program in PARI for (b) and (c), and if possible attach a printout.)
   (a) $11^x \underset{(71)}{\equiv} 21$
   (b) $156^x \underset{(593)}{\equiv} 116$
   (c) $650^x \underset{(3571)}{\equiv} 2213$.

[4] described at length in [HPS]

(4) Write out your own proof that the Pohlig-Hellman algorithm works in the particular case that $p - 1 = q_1 \cdot q_2$ is a product of two distinct primes. (This needn't be long – half a page or so.)
(5) Use Pohlig-Hellman to solve the discrete log problem $7^x \underset{(433)}{\equiv} 166$.

CHAPTER 15

RSA Cryptosystem

So far we have discussed Diffie-Hellman and El Gamal, which rely for their security upon the supposed difficulty of the Discrete Logarithm Problem. Now we turn to an encoding scheme which is based on the difficulty of finding roots.

What difficulty, you might ask? If p is an odd prime, we had the result that $x^k \underset{(p)}{\equiv} a$ is soluble (with $(k, p-1)$ solutions) $\iff$ $a^{\frac{p-1}{(k,p-1)}} \underset{(p)}{\equiv} 1$. Moreover, if $(k, p-1) = 1$ and $\ell \cdot k \underset{(p-1)}{\equiv} 1$, then little Fermat implies $(a^\ell)^k = a^{\ell k} = a^{\mu(p-1)} \cdot a \underset{(p)}{\equiv} a$, making $x = a^\ell$ a solution. Using the Euclidean algorithm and fast-powering, ths poses no *difficulty* at all!!

More generally, if

$$n > 1,\ (a, n) = 1,\ \text{and}\ (k, \phi(n)) = 1,$$

then we can solve the congruence

$$x^k \underset{(n)}{\equiv} a$$

by:

- computing $\phi(n)$;
- finding $e, f \in \mathbb{N}$ such that $1 = e \cdot k - f \cdot \phi(n)$ ($\implies$ $e \cdot k \underset{\phi(n)}{\equiv} 1$);
- computing a^e by fast powering.

This gives our x, since

$$(a^e)^k = a^{f \cdot \phi(n)+1} = (a^{\phi(n)})^f a \underset{(n)}{\equiv} a.$$

The difficulty is concealed in the first step, computing $\phi(n)$, since this involves knowing a factorization of n. We will focus on the specific case:

THEOREM 147. *Let p, q be distinct primes, $a \in \mathbb{Z}$, and $(k, (p-1)(q-1)) = 1$. Take e to be an inverse of k mod the lcm $[p-1, q-1]$. Then $x = a^e \pmod{pq}$ is a solution to $x^k \underset{(pq)}{\equiv} a$.*

PROOF. Suppose $(a, pq) = 1$. (The general case is an exercise.) Set $\ell = [p-1, q-1] = \ell' \cdot (q-1) = (p-1) \cdot \ell''$. We have by Fermat

$$a^{ek} = a^{\mu\ell+1} = \begin{cases} (a^{p-1})^{\mu\ell''} a \underset{(p)}{\equiv} a \\ (a^{q-1})^{\mu\ell'} a \underset{(q)}{\equiv} a \end{cases} \overset{\text{CRT}}{\Longrightarrow} a^{ek} \underset{(pq)}{\equiv} a.$$

□

We are now ready to describe the

RSA Algorithm. (**S** = Sender, **R** = Receiver)

- **R** chooses 2 large primes p, q and produces $n = pq$;
- **R** also chooses an exponent k coprime to $\phi(n) = (p-1)(q-1)$;
- **R** computes an inverse e of k in $\mathbb{Z}/\phi(n)\mathbb{Z}$ or (better, since easier) $\mathbb{Z}/[p-1, q-1]\mathbb{Z}$;
- **R** makes the key (n, k) public;
- **S** encodes a message m as $c := m^k \pmod{n}$, and sends it to **R**;
- **R** decodes the message by computing $c^e (= m^{ke}) \underset{(pq)}{\equiv} m$.

Note how this uses Theorem 147 at the end.

EXAMPLE 148. $p = 17$, $q = 19$, $n = pq = 17 \cdot 19 = 323 \implies \phi(n) = 16 \cdot 18 = 288$. Now $k = 95 (= 5 \cdot 19)$ is coprime to 288, which yields the public key $(323, 95)$. An inverse of k mod 288 is 191 (by Euclidean algorithm). [Better: an inverse of k mod $[16, 18] = 144$ is 47.] Someone encodes the letter "X" (as $m = 24$) via $c = m^{95} = 24^{95} \underset{(323)}{\equiv} 294$. We decode the message by $294^{47 (\text{or } 191)} \underset{(323)}{\equiv} 24$.

For longer messages, it is much safer to encode several letters as a block, rather than encoding letters individually (which would be susceptible to a frequency analysis). Below we will explore some other possible "attacks" on the RSA cryptosystem. Note that it is sufficient for the "**I**nterceptor" to factor n.

Attack 1: If we know n and $\phi(n)$ (or $p+q$), then we can easily factor n. (Here I'm assuming as above that $n = pq$.)

METHOD: We have

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1,$$

hence

$$p + q = n - \phi(n) + 1.$$

Now, p and q are roots of the quadratic equation

$$0 = (x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - (n - \phi(n) + 1)x + n.$$

Of course, we can easily solve this equation . . . □

EXAMPLE 149. Suppose we know $n = 437$ is the product of 2 primes and $\phi(n) = 396$. The roots of

$$x^2 - \underbrace{(n - \phi(n) + 1)}_{42} x + 437 = 0$$

are given by

$$x_\pm = 21 \pm \sqrt{21^2 - 437} = 21 \pm 2.$$

Attack 2: ("Fermat factorization method") If p and q are "close", we can find the factorization of $n = pq$.

METHOD: Assume $p > q$, so that $s = \frac{p-q}{2}$ is small relative to $t = \frac{p+q}{2}$, which is close to $\sqrt{n}$. Now consider the difference of squares:

$$\begin{aligned} t^2 - s^2 &= \left(\tfrac{p+q}{2}\right)^2 - \left(\tfrac{p-q}{2}\right)^2 \\ &= \tfrac{1}{4}\left(p^2 + 2pq + q^2 - (p^2 - 2pq + q^2)\right) \\ &= pq = n. \end{aligned}$$

So: the idea is to test whether $t^2 - n$ is a square for $t - \sqrt{n} > 0$ small. Eventually, you reach one (and this is s^2). □

EXAMPLE 150. $p = 1201, q = 1409 \to n = 1692209$. Now $\lceil \sqrt{n} \rceil = 1301$, so we take (on a computer) square roots of $1301^2 - n$, $1302^2 - n$, etc. until we get what appears to be an integer. This happens at $1305^2 - n = 10816 = 104^2$. So $t = 1305$, $s = 104$, and we recover $p = t + s = 1409$, $q = t - s = 1201$.

Attack 3: Why the **R**eceiver should never publish two exponents for the same public modulus n.

METHOD: Say **R** makes (n, k_1) and (n, k_2) public, and **S** uses both of them to encode a message, sending

$$c_1 = m^{k_1} \pmod{n} \quad \text{and} \quad c_2 = m^{k_2} \pmod{n}.$$

The **I**nterceptor can compute A, B satisfying $Ak_1 + Bk_2 = \gcd(k_1, k_2)$ and then write

$$c_1^A c_2^B = m^{Ak_1 + Bk_2} = m^{(k_1, k_2)},$$

which is m itself if $(k_1, k_2) = 1$!! □

Attack 4: Why **R** should find another way to authenticate his or her identity than by willingly decrypting ciphertexts.

METHOD: As **I**, you can take a ciphertext c which you have intercepted, and multiply by some arbitrary nonsense message μ encoded by the public key (n, k), sending the result

$$c' := \mu^k \cdot c \pmod{n}$$

to **R**. Now **R** "decrypts" c' via

$$(c')^e = \mu^{ek} \cdot c^e = \mu \cdot m$$

(where we have used Theorem 147 twice) and sends this back. Now you compute $(\mu m) \cdot \mu^{-1} = m$. □

In Attacks 1-2, **I** breaks the code by factoring n; it isn't known whether this is really necessary (cf. [HPS, p. 122]).

Exercises

(1) Let p and q be distinct primes, and let e and d be integers satisfying $de \underset{\ell}{\equiv} 1$ (where ℓ is the lcm $[p-1, q-1]$). Suppose further that c is an integer with gcd $(c, pq) > 1$. Prove that $x \underset{(pq)}{\equiv} c^d$ is a solution to the congruence $x^e \underset{(pq)}{\equiv} c$, thereby completing the proof of Theorem 147.

(2) Your RSA modulus is $n = 91$ and your encoding exponent is $e = 19$. Find the decryption exponent d. Why would $e = 9$ be a bad choice?

(3) Here is a cryptosystem which is supposed to be faster than RSA (and was apparently proposed at a cryptography conference): **(1)** Alice chooses two large primes p and q and publishes $N = pq$, then chooses 3 random numbers g, r_1, r_2 mod N and computes $g_1 \underset{(N)}{\equiv} g^{r_1(p-1)}$ and $g_2 \underset{(N)}{\equiv} g^{r_2(q-1)}$. Her public key is the triple (N, g_1, g_2) and her private key is (p, q). **(2)** Bob wants to send the message m (mod N) to Alice. He chooses two random numbers s_1 and s_2 (mod N), computes $c_1 \underset{(N)}{\equiv} m g_1^{s_1}$ and $c_2 \underset{(N)}{\equiv} m g_2^{s_2}$, and sends the ciphertext (c_1, c_2) to Alice. **(3)** Alice uses the CRT to solve the pair of congruences $x \underset{(p)}{\equiv} c_1$ and $x \underset{(q)}{\equiv} c_2$. (This part is faster than RSA for sure.)
   (a) Prove that Alice's solution x is equal to Bob's plaintext m.
   (b) Explain why this cryptosystem is not secure. (Oops.)

(4) Formulate a man-in-the-middle attack, similar to the one we described for Diffie-Hellman, for the RSA cryptosystem.

CHAPTER 16

Introduction to PARI

Besides the huge, expensive packages like Mathematica, Maple, and MAGMA, there are a number of free "calculators" which are useful in a particular area of mathematics: e.g. LiE and ATLAS for representation theory; the SAGE cloud for algebra, combinatorics, and number theory; and Wolfram Alpha for quick online computations across a wide range. PARI/GP is a computer algebra system for fast computations in number theory. It was originally designed by Henri Cohen, who literally wrote the book[1] on computational number theory. You will want to install it on your computer from

`http://pari.math.u-bordeaux.fr/`

in order to do some of the exercises.

Below I have copied some commands and very simple "programs" to illustrate how PARI is used. You will also want to have a look at

- K. Conrad, "Introduction to PARI",
- W. Stein, "Elementary number theory" (Lectures 3 and 16), and
- the official PARI tutorial and reference card.

The "`?`" (or "`gp >`") is GP's command prompt. Outputs are not displayed below (only the inputs). Expressions enclosed in brackets "[]" are not PARI code.

Checking the prime number theorem:

```
?       pi(x,c=0) = forprime(p=2,x,c++);c;
?       for(n=1,10,print(n*1000," ",pi(n*1000)," ",n*1000/(log(n*1000)-1)))
```

[1] H. Cohen, "A Course in Computational Number Theory" Springer, 1993.

Primality testing: Wilson's theorem:

```
?       Wilson(n) = Mod((n-1)!,n) == Mod(-1,n)
?       Wilson(5)
?       Wilson(10)
```

Primality testing: Fermat's theorem:

```
?       probprime(n,a) = Mod(a,n)^(n-1) == Mod(1,n)
?       x = [huge odd number]
?       for(i=0,100,if(probprime(x+2*i,2),print(i)))
?       [do some with a=3, 4, etc.]
```

Discrete log:

```
?       dislog(x,g,s)=s=g; for(n=1,znorder(g),if(x==s,return(n),s=s*g));0;
?       dislog(18,Mod(5,23))
?       p=nextprime(9048610000)
?       g=Mod(5,p)
?       a=g^948603
?       dislog(a,g) [takes a moment]
?       znlog(a,g) [much faster, built-in optimized version]
```

Primitive roots:

```
?       roots(p) = for(n=1,p-1,if(znorder(Mod(n,p))==(p-1),print1(n," ")))
?       roots(17)
?       roots(19)
```

Diffie-Hellman key exchange:

[Notes: in $a = qb + r$, "a\b" is the q, and "a%b" is the r; "!" means "not"; and "? ***" explains the command "***".]

```
?       p=nextprime([huge 30 digit number])
?       isprime((p-1)\2)
?       nextgoodprime(p) = while(!isprime((p-1)\2),p=nextprime(p+1));p
?       nextgoodprime(p)
?       g=2
?       znorder(Mod(g,p))
?       ?random
?       Alice=random(p)
```

```
?       Bob=random(p)
?       Alice_say = Mod(g,p)^Alice
?       Bob_say = Mod(g,p)^Bob
?       secret = Alice_say^Bob
?       Bob_say^Alice
```

RSA Attack 2: factoring a product of "close" primes:

```
?       n=1692209
?       for(i=0,10,print(i,“ ”,sqrt((floor(sqrt(n))+i+1)^2 - n)))
```

Exercises

(1) Artin conjectured that the number of primes $p \leq x$ such that 2 is a primitive root mod p is asymptotic to $C\pi(x)$ for some constant C. (Recall it is still not even proved if there are infinitely many p having 2 as primitive root.) Using PARI, make an educated guess as to what "Artin's constant" C should be, to a few decimal places of accuracy. Explain your reasoning. (Of course, don't try to prove that your guess is correct.)

CHAPTER 17

Breaking RSA

We discussed a few attacks on RSA in §III.D, all fairly superficial,[1] which relied either on unforced errors by the Sender and Receiver or on factoring N. Now it is time to push this a bit further to understand possible security issues. RSA is often presented with the warning that computing roots mod $pq = N$ — the essence of breaking RSA — may not be as hard as factoring N. However, there is an important counterargument here: finding a decryption exponent essentially *is* tantamount to factoring N, in a sense we now describe.

Factoring an RSA modulus, v. 1.0. Let (n, e) be an RSA public key, where $n = pq$ is a product of distinct primes, and e is the encryption exponent. Suppose you have obtained the decryption exponent d, which satisfies $a^{de} \underset{(n)}{\equiv} a$ $(\forall a)$. Write $m := de - 1$, and note that

$$(-1)^m = (-1)^{de} \cdot (-1) \underset{(n)}{\equiv} (-1)^2 = 1$$

implies that m is even.

Now pick some a, say with $(a, n) = 1$. The idea now is to compute successive square roots of $a^m \pmod{n}$, i.e.

$$a^{\frac{m}{2}} \pmod{n},\ a^{\frac{m}{4}} \pmod{n},\ \text{etc.}$$

until

$$a^{\frac{m}{2^k}} \underset{\not\equiv}{(n)} 1. \tag{25}$$

If this doesn't happen for your choice of a, throw it under the bus and choose another.

[1] though the difference of squares trick can be made quite sophisticated; cf. [HPS, §3.6].

Assuming (25), there are three possibilities:

- $a^{\frac{m}{2^k}} \underset{(p)}{\equiv} 1, a^{\frac{m}{2^k}} \underset{(q)}{\not\equiv} 1 \; (\underset{\text{(why?)}}{\Longrightarrow} a^{\frac{m}{2^k}} \underset{(q)}{\equiv} -1)$
- $a^{\frac{m}{2^k}} \underset{(q)}{\equiv} 1, a^{\frac{m}{2^k}} \underset{(p)}{\not\equiv} 1 \; (\Longrightarrow a^{\frac{m}{2^k}} \underset{(p)}{\equiv} -1)$
- $a^{\frac{m}{2^k}} \underset{(q)}{\not\equiv} 1, a^{\frac{m}{2^k}} \underset{(p)}{\not\equiv} 1.$

There is a good chance that one of the first two holds, assume (say) the first. Then we have

$$p \mid (a^{\frac{m}{2^k}} - 1) \, , \quad q \nmid (a^{\frac{m}{2^k}} - 1)$$

$\Longrightarrow (a^{\frac{m}{2^k}} - 1, n) = p$. In other words, computing $a^{\frac{m}{2^k}} \pmod n$ followed by the Euclidean algorithm (to compute the gcd) gives us a prime factor of n.

EXAMPLE 151. The public key is $(n, e) = (10403, 7)$, and your spy delivers $d = 8743$. You compute $m = de - 1 = 61200$. Now take $a = 5$, and noting that $61200 = 2^4 \cdot 3825$, try $k = 1, 2, 3, 4$. We find $a^{\frac{m}{2^k}} \underset{(n)}{\equiv} 1$ for $k = 1, 2, 3$, but $a^{3825} \underset{(n)}{\equiv} 102$, and the gcd $(a^{3825} - 1, n) = (101, 10403) = 101$. Conclude that $n = 101 \cdot 103$.

Factoring an RSA modulus, v. 2.0 (Pollard $p - 1$ algorithm). This time I will begin with the formal algorithm. Let n be the integer we wish to factor (assumed to be of the form pq), and pick $M \in \mathbb{N}$ (relatively small).

(1) Set $a = 2$;
(2) Loop $j = 2, 3, 4, \ldots, M$;
(3) Set $a = a^j \pmod n$;
(4) Compute $d = (a - 1, n)$;
(5) If $d \neq 1, n$ print d, stop;
(6) Return to step 2 (if $j < M$);
(7) Increment a, return to Step (1).

Claim: If $p - 1$ is a product of small primes but $q - 1$ is not, this algorithm will "quickly" produce the factorization of n (i.e., it will stop in some iteration of Step (5)).

An immediate consequence is that when choosing p and q for RSA, one should check that $p-1$ and $q-1$ are not products of small primes (which can be done very quickly).

"PROOF" OF CLAIM: In the algorithm, we are computing

$$d_j = (a^{j!} - 1, n)$$

where (asabove) $a^{j!} - 1$ need only be computed mod n. Suppose $p - 1 = p_1^{r_1} \cdots p_s^{r_s}$ (p_i distinct primes), $m = \max\{r_1 p_1, \ldots, r_s p_s\}$,[2] and $q - 1$ has at least one (prime) factor larger tham m. Then

$$(p-1) \mid m!\,, \quad (q-1) \nmid m!.$$

Since q is prime, $\mathbb{Z}_q^*$ has a generator α, with the property that $\alpha^\mu \underset{(q)}{\equiv} 1 \iff (q-1) \mid \mu$. As p is prime, $(p-1) \mid \mu \implies \alpha^\mu \underset{(p)}{\equiv} 1$ as long as $(\alpha, p) = 1$. Taking a to be a smal ($\implies$ not divisible by p) generator of $\mathbb{Z}_q^*$, we get $p \mid (a^{m!} - 1)$ and $q \nmid (a^{m!} - 1) \implies (a^{m!} - 1, n) = (a^{m!} - 1, pq) = p$. □

EXAMPLE 152. $n = 10403$, $a = 2$. Compute (mod n)

$$2 \overset{(\cdot)^2}{\to} 4 \overset{(\cdot)^3}{\to} 64 \overset{(\cdot)^4}{\to} \cdots \overset{(\cdot)^{10}}{\to} 9798$$

so $(a^{10!} - 1, n) = (9797, 10403) = 101$ (using the EA). Why does it work? Because

$$p - 1 = 101 - 1 = 2^2 \cdot 5^2 \ (\implies m = 10)$$

while

$$q = 1 = 103 - 1 = 102 = 17 \cdot 3 \cdot 2.$$

Probabilistic encryption. If your space of plaintexts is small — e.g. you are sending a binary message like 0 (= no/we lost) or 1 (= yes/we won) — then the Interceptor can simply encode the possibilities by the public key, and decide (by composing these with the ciphertext the Sender broadcasts) what the message is. This is a major

[2] remark that fast powering computes $a^{m!} \sim (\frac{m}{e})^m$ in $\sim 2\log_2((\frac{m}{e})^m) \simeq 2m\log_2 m$ steps, not very long at all.

problem with the RSA algorithm, though not as much for El Gamal — because the *ephemeral key* chosen by the Sender means there are *many* possible ciphertexts for each plaintext. One says that El Gamal is a *probabilistic cryptosystem*.

Another (less practical, but more amusing) probabilistic encoding scheme, called **Goldwasser-Micali**, is based on quadratic residues and the Jacobi symbol.

- **R**eceiver chooses primes p and q, and a with
$$\left(\frac{a}{p}\right) = -1 = \left(\frac{a}{q}\right),$$
sets $n = pq$.
- **R** broadcasts (n, a) = public key.
- **S**ender chooses plaintext $m \in \{0, 1\}$, and a *random* $r \in \mathbb{Z} \cap (1, n)$.
- **S** computes ciphertext
$$c = \begin{cases} r^2 \pmod{n}, & \text{if } m = 0 \\ ar^2 \pmod{n}, & \text{if } m = 1 \end{cases}$$
and sends to **R**.
- **R** decrypts the message by the formula
$$m = \begin{cases} 0, & \text{if } \left(\frac{c}{p}\right) = 1 \\ 1, & \text{if } \left(\frac{c}{p}\right) = -1. \end{cases}$$
(Remember, p is known only to **R**.)

This works, because if $m = 0$ then
$$\left(\frac{c}{p}\right) = \left(\frac{r^2}{p}\right) = 1$$
while if $m = 1$ then
$$\left(\frac{c}{p}\right) = \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{r^2}{p}\right) = \left(\frac{a}{p}\right) = -1.$$

Moreover, in either case

$$\left(\frac{c}{n}\right) = \begin{cases} \left(\frac{r^2}{n}\right) &= 1 \\ \left(\frac{ar^2}{n}\right) &= \left(\frac{a}{n}\right)\left(\frac{r^2}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = (-1)^2 = 1 \end{cases}$$

so the Interceptor really will have to factor N to break the code.

Exercises

(1) The ciphertext 5859 was obtained using the RSA algorithm with public key $(n, e) = (11413, 7467)$. Find the original plaintext message (a number less than 11413) from which it was obtained. [Hint: factorize 11413 and then produce a decryption exponent.]

(2) Show that if $x^2 \underset{(n)}{\equiv} y^2$ and x is not equivalent to $\pm y \pmod{n}$, then $(x + y, n)$ is a non-trivial factor of n.

(3) A *decryption exponent* for an RSA public key (N, e) is an integer d with the property that $a^{de} \underset{(N)}{\equiv} a$ for all integers a with $(a, N) = 1$. Let $N = 38749709$. Eve's magic box tells her that the encryption exponent $e = 10988423$ has decryption exponent $d = 16784693$ and that the encryption exponent $e = 25910155$ has decryption exponent $d = 11514115$. Use this information to factor N.

(4) Use Pollard $p - 1$ method to factor $n = 48356747$.

(5) Suppose that the plaintext space $\mathcal{M}$ of a certain cryptosystem is the set of bit strings of length $2b$. Let e_k and d_k be the encryption and decryption functions associated with a key $k \in \mathcal{K}$. This exercise describes one method of turning the original cryptosystem into a probabilistic cryptosystem.

Alice sends Bob an encrypted message by performing the following steps:

(1) Alice chooses a b-bit message m' to be encrypted.

(2) Alice chooses a string r consisting of b random bits.

(3) Alice sets $m = r \parallel (r \oplus m')$, where $\parallel$ denotes concatenation and $\oplus$ denotes XOR. Notice that m has length $2b$ bits.

(4) Alice computes $c = e_k(m)$ and sends the ciphertext c to Bob.

(a) Explain how Bob decrypts Alice's message and recovers the plaintext m'. (We assume that Bob knows the decryption function d_k.)
(b) If the plaintexts and the ciphertexts of the original cryptosystem have the same length, what is the *message expansion ratio* of the new probabilistic cryptosystem? (If a b-bit message gets converted to a μb-bit message, this ratio is μ by definition.)
(c) More generally, is the original cryptosystem has a message expansion ratio of μ, what is the message expansion ratio of the new probabilistic cryptosystem?

Part 4

Diophantine equations

CHAPTER 18

A first view of Diophantine equations

Diophantine equations are polynomial equations with integer coefficients (and any number of variables) to which solutions are sought *in integers*. A famous (and recent!) results that should immediately comes to mind is "Fermat's last [i.e. Wiles's] Theorem"

$$x^n + y^n = z^n\,,\ n > 2\,,\ x, y, z \in \mathbb{Z} \quad \Longrightarrow \quad xyz = 0.$$

We will mainly concentrate on quadratic (degree 2) and cubic (degree 3) equations.

First some history: **Hilbert's 10th problem** (1900) asks for an algorithm whcih determines (in a finite number of operations) whether a given Diophantine equation is soluble (in integers). In 1970 — building on at least four decades of work (of Hilary Putnam, Martin Davis, and especially Julia Robinson[1]), some of it in logic and analytic philosophy — Yuri Matiyasevich proved that such an algorithm does not in general exist. (His method involved the famous Fibonacci numbers, and so-called "Diophantine sets".) There exist, for example, Diophantine equations with no solutions, but such that this fact *cannot be proved* ("within a given axiomatization of number theory"). This may be viewed as a "concrete" instance of Gödel's Incompleteness Theorem.

So while Diophantine equations withhold their secrets from any method, it is certainly true that algebraic number theory has been tremendously successful in making them more accessible — a case

[1] see the documentary *Julia Robinson and Hilbert's 10th problem*

in point will be our study of Pell's equation

$$x^2 - y^2 d = \begin{cases} \pm 1 & \text{if } d \underset{(4)}{\equiv} 2,3 \\ \pm 4 & \text{if } d \underset{(4)}{\equiv} 1 \end{cases} \quad (d \text{ squarefree}).$$

But we shall begin instead with a pair of fun examples to introduce the topic.

Lagrange's four-square theorem. I claim that for any $N \in \mathbb{N}$, there exist $w, x, y, z \in \mathbb{Z}$ such that

$$N = x^2 + y^2 + z^2 + w^2;$$

that is, N is a "4-square". (Note that any of x, y, z, w are allowed to be 0.)

EXAMPLE 153. $111 = 9^2 + 5^2 + 2^2 + 1^2$, and $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Step 1: Reduction to N prime. An identity of Euler

(26)
$$(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) = (aw+bx+cy+dz)^2 + (ax-bw-cz+dy)^2 + (ay+bz-cw-dx)^2 + (az-by+cx-dw)^2$$

says that any product of 4-squares is again a 4-square. So it is sufficient to prove the 4-square theorem for (odd) primes p.

Step 2: For each odd prime p, there exists $0 < m < p$ such that mp is a 4-square. More precisely, we will show that $mp = x^2 + y^2 + 1$ for some $x, y \in \mathbb{Z}$ and $0 < m < p$. You see, either -1 is a square (mod p), and we can take $x = 0$; *or* the set of $\frac{p+1}{2}$ numbers (mod p) $-1 - y^2$ and $\frac{p+1}{2}$ numbers (mod p) x^2 must have an intersection, by the pigeonhole principle. [Details are left as an exercise.]

Step 3: If mp is a 4-square, then there exists $0 < m' < m$ such that $m'p$ is a 4-square. (Then we will be done, since by repeatedly applying this we eventually get $m' = 1$.)

Case I (m even): If $2N = w^2 + x^2 + y^2 + z^2$, then there are an even number of odd integers and an even number of even integers

amongst x, y, z, w. Group them in pairs accordingly, say $x \underset{(2)}{\equiv} w$, $y \underset{(2)}{\equiv} z$. Then

$$N = \left(\tfrac{w+x}{2}\right)^2 + \left(\tfrac{w-x}{2}\right)^2 + \left(\tfrac{y+z}{2}\right)^2 + \left(\tfrac{y-z}{2}\right)^2$$

presents N as a 4-square. In particular, if mp is a 4-square, then so is $\frac{m}{2}p$.

Case II (m odd): Given $mp = w^2 + x^2 + y^2 + z^2$, with $0 < m < p$ (see Step 2), choose the unique $a, b, c, d \underset{(m)}{\equiv} w, x, y, z$ with $-\frac{m}{2} < a, b, c, d < \frac{m}{2}$. Then we have

$$a^2 + b^2 + c^2 + d^2 \underset{(m)}{\equiv} w^2 + x^2 + y^2 + z^2 \underset{(m)}{\equiv} 0$$

$$\implies a^2 + b^2 + c^2 + d^2 = mk,$$

for some $0 < k < m$. (If $k \geq m$, this contradicts $|a, b, c, d| < \frac{m}{2}$; if $k = 0$, then $0 = a = b = c = d \implies m \mid x, y, z, w \implies m^2 \mid x^2 + y^2 + z^2 + w^2 = mp \implies m \mid p$ contradicting $0 < m < p$.)

Now we use Euler's identity (26) again, in which the left-hand side equals $(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = km \cdot mp$. The right-hand side is a sum squares of four expressions, each divisible by m: e.g.

$$aw + bx + cy + dz \underset{(m)}{\equiv} a^2 + b^2 + c^2 + d^2 = mk \underset{(m)}{\equiv} 0,$$

$$ax - bw - cz + dy \underset{(m)}{\equiv} ab - ba - cd + dc = 0.$$

Therefore

$$kp = X^2 + Y^2 + Z^2 + W^2,$$

where $k < m$. This finishes Step 3 hence the proof of Lagrange's Theorem.

Fermat's Last Theorem with $n = 4$. I make the slightly stronger claim that

$$X^4 + Y^4 = Z^2 \tag{27}$$

has no solution in (all nonzero) integers. Clearly it suffices to show there is no solution in positive integers. In fact, it suffices to prove there is no primitive solution — that is, a solution (x, y, z) with $x, y, z > 0$ and $\gcd(x, y, z) = 1$. For if a positive solution (X, Y, Z) exists with $p \mid X, Y, Z$, then actually $p^2 \mid Z$ and $(\frac{X}{p}, \frac{Y}{p}, \frac{Z}{p^2})$ is a new solution; repeating this, one eventually arrives at a primitive one.

So suppose we have a primitive solution (x, y, z). Writing it as $(x^2)^2 + (y^2)^2 = z^2$, this is a Pythagorean triple. In §IV.B we will prove that the complete list of Pythagorean triples $a^2 + b^2 = c^2$ is $\{(2rs, s^2 - r^2, s^2 + r^2) \mid r, s \in \mathbb{N}\}$. So there must be integers r, s with $s > r$ such that

$$x^2 = 2rs,\ y^2 = s^2 - r^2, \text{ and } z = s^2 + r^2.$$

From the primitivity assumption it also follows that $(r, s) = 1$, and $(y, z) = 1$ (since any prime dividing y and z also would divide x).

We rewrite (27) as

$$x^4 = (z - y^2)(z + y^2) \left(= 2r^2 \cdot 2s^2\right). \tag{28}$$

Suppose $r \in \mathbb{N}$ divides both factors on the right-hand side of (28). Then

$$r \mid z - y^2 + z + y^2 = 2z \text{ and } r \mid z + y^2 - (z - y^2) = 2y^2 \quad \Longrightarrow \quad r \mid 2,$$

and so $(z - y^2, z + y^2) = 2$ (and not $2^{k>1}$). Using (28) again, we find

(a) $z - y^2 = 2a^4$ (a odd) and $z + y^2 = 2^3 b^4$; or

(b) $z - y^2 = 2^3 a^4$ and $z + y^2 = 2b^4$ (b odd).

If (a) holds, then $2y^2 = 2^3 b^4 - 2a^4 \implies y^2 = 4b^4 - a^4 \underset{(4)}{\implies} y^2 \equiv -a^4 \underset{(4)}{\equiv} -1$, which is impossible as -1 is not a quadratic residue mod 4.

So (b) holds (with both a and b nonzero), and adding/subtracting equations yields

$$y^2 = b^4 - 4a^4$$
$$z = b^4 + 4a^4,$$

which imply

$$4a^4 = (b^2 - y)(b^2 + y) \quad 0 < b < z. \tag{29}$$

Suppose some prime p divides $b^2 - y$ and $b^2 + y$. Then $p \mid 2b^2$ and $p \mid 2y$. If $p \neq 2$ then p divides y and $2b^4 - y^2 = z$, hence also $z - y^2$ and $z + y^2$, which contradicts $(z - y^2, z + y^2) = 2$. So $p = 2$, and $(b^2 - y, b^2 + y) = 2$. (It can't be $2^{k>1}$, since b is odd.)

So we can rewrite (29) as

$$a^4 = \left(\tfrac{b^2-y}{2}\right)\left(\tfrac{b^2+y}{2}\right)$$

with the right-hand factors relatively prime (and nonzero). By the fundamental theorem of arithmetic, we conclude from this that $b^2 - y = 2c^4$ and $b^2 + y = 2d^4$, and so

$$b^2 = c^4 + d^4\,, \quad \text{where } 0 < b < z. \tag{30}$$

In fact, since c and d are coprime and nonzero (we may take them to be positive), (c, d, b) is a second primitive solution to (27), like the solution (x, y, z) we started with. But there is an important difference: b is *smaller* than z.

This is the end of the proof: we could always have taken (x, y, z) to be a primitive solution with minimal $z\,(> 0)$. The *method of descent* just described (and essentially due to Fermat) then produces a primitive solution with smaller $z\,(> 0)$, which is absurd. Consequently, there can't have been a primitive solution, hence any solution in nonzero integers, in the first place.

CHAPTER 19

Quadratic Diophantine equations

We now begin the more systematic investigation of equations of degree two and three.[1]

The equation $x^2 + y^2 = z^2$ (Pythagorean triples). First note that from any solution we get infinitely many by $(kx, ky, , kz)$, $k \in \mathbb{Z}$.

DEFINITION 154. A triple $(a, b, c) \in \mathbb{Z}^3$ is *primitive* if $\gcd(a, b, c) = 1$, and *Pythagorean* if $a^2 + b^2 = c^2$.

We shall now find all primitive Pythagorean triples. First, we cannot have $a, b, c \underset{(2)}{\equiv} 0$ (since the gcd is 1); and so a and b cannot both be even (otherwise, c would be). If a and b were both odd, then $a^2 + b^2 \underset{(4)}{\equiv} 1 + 1 = 2$; but $c^2 \underset{(4)}{\equiv} 2$ is impossible! Without loss of generality we can therefore assume a even and b odd, hence c odd.

Next, put $a = 2n$, and note that

$$a^2 = c^2 - b^2 = (\underbrace{c - b}_{\text{even}})(\underbrace{c + b}_{\text{even}}).$$

Put $c - b = 2v$, $c + b = 2w$; we then have

$$(2n)^2 = 2v \cdot 2w$$

hence

$$n^2 = vw \tag{31}$$

where $n, v, w \neq 0$. If a prime $g \mid v, w$, then g divides $w - v = b$ and $w + v = c$, which gives $g \mid a$, a contradiction. Therefore $(v, w) = 1$.

But if v and w have no common prime factors, the Fundamental Theorem of Arithmetic (unique factorization in $\mathbb{Z}$) together with

[1] For degree one, see the material on linear Diophantine equations in [NZM].

equation (31) imply $v = r^2$ and $w = s^2$. We conclude that $b = w - v = s^2 - r^2$, $c = w + v = s^2 + r^2$, and $a^2 = 4n^2 = 4vw = 4r^2s^2 = (2rs)^2 \implies a = 2rs$. Conversely, we can check that each such triple is Pythagorean (try it!), proving the

THEOREM 155. *The complete list of primitive Pythagorean triples is*

$$\left\{(2rs, s^2 - r^2, s^2 + r^2) \mid r, s \in \mathbb{Z}\backslash\{0\};\ (r,s) = 1;\ r, s \text{ not both odd}\right\}.$$

(*To get all Pythagorean triples, change the conditions on r, s to just "$r, s \in \mathbb{Z}$".*)

REMARK 156. It is easy to see that $(r,s) = 1 \implies$ no odd prime factor of r can divide $s^2 - r^2$ or $s^2 + r^2$. But what about 2? 2 divides $2rs$, and will divide $s^2 \pm r^2 \iff s$ and r are both even or both odd. If $(r,s) = 1$ they can't both be even.

EXAMPLE 157. $r = 40$ and $s = 81$ give $(a,b,c) = (6480, 4961, 8161)$. So $4961^2 + 6480^2 = 8161^2$ (apparently written down by the Babylonians!).

The equation $c^2 - b^2 = n$.. We shall seek, for given n (e.g. a^2 in the Pythagorean equation), the *number* of solutions to this one.

DEFINITION 158. $\sigma_k(n) := \sum_{d|n} d^k$ (for $n \in \mathbb{N}$), so in particular $\sigma_0(n)$ is the number of positive divisors of n.

The table

n	1	2	3	4	5	6	7	8	9	10
$\sigma_0(n)$	1	2	2	3	2	4	2	4	3	4

suggests

LEMMA 159. *$\sigma_0(n)$ odd $\iff$ n is a square.*

PROOF. Factors come in pairs d and $\frac{n}{d}$, unless (when $d = \sqrt{n}$) n is a square. □

LEMMA 160. $\sigma_0(p^m) = m + 1$.

PROOF. Since this is obvious, I'll prove that a cow has nine legs instead. A cow has four more legs than no cow. No cow has five legs. Done. □

LEMMA 161. *σ_0 is multiplicative: $(m,n) = 1 \implies \sigma_0(mn) = \sigma_0(m)\sigma_0(n)$.*

PROOF. The divisors of mn are de where $d \mid m$ and $e \mid n$. In fact, the correspondence between such pairs (d,e) and divisors of mn is bijective: for if (d',e') is another such pair, and $d'e' = de$, then $(m,n) = 1 \implies (e',d) = 1 = (e,d') \implies d' = d$ and $e' = e$. □

So if we write $n = \prod p_i^{m_i}$ as a product of powers of distinct primes, then

$$\sigma_0(n) = \prod_i (m_i + 1).$$

Now suppose (x,y) is a solution to our equation, with $x, y > 0$. Put $d = x + y$, $e = x - y$, so that $de = n$. Since $d + e = 2x$, $d \underset{(2)}{\equiv} e$; and since $d - e = 2y > 0$, $d > e$. Hence

$$(x,y) \in \mathscr{S} := \left\{ \left(\tfrac{d+e}{2}, \tfrac{d-e}{2} \right) \middle| d > e > 0,\ de = n,\ d \underset{(2)}{\equiv} e \right\},$$

and conversely each element of $\mathscr{S}$ provides a solution.

THEOREM 162. *The number of elements in $\mathscr{S}$ is*

$$|\mathscr{S}| = \begin{cases} \frac{1}{2}\sigma_0(n) & \text{if } n \text{ odd nonsquare}, \\ \frac{\sigma_0(n)-1}{2} & \text{if } n \text{ odd square}, \\ \frac{1}{2}\sigma_0(\frac{n}{4}) & \text{if } n \text{ even nonsquare} \quad (\text{div. by } 4), \\ \frac{\sigma_0(\frac{n}{4})-1}{2} & \text{if } n \text{ even square} \quad (\text{div. by } 4). \end{cases}$$

If n is even but $4 \nmid n$, then $|\mathscr{S}| = 0$.

PROOF. (n odd) If $de = n$, then $d \,(\underset{(2)}{\equiv} 1) \underset{(2)}{\equiv} e$ is automatic. Furthermore, d determines e. So $|\mathscr{S}|$ is the number of divisors of n with $d > \frac{n}{d}$, i.e. $d > \sqrt{n}$. Of course, e is in each case $\frac{n}{d}$, and if n is a square then we miss out on $d = \sqrt{n} = e$.

(n even) If $de = n$, then one (hence both) of d and e must be even. So $4 \mid n$ (otherwise there is no solution, and $|\mathscr{S}| = 0$). In this case, $d = 2d'$, $e = 2e'$ and $d'e' = \frac{n}{4}$; $\mathscr{S}$ identifies with

$$\left\{(d' + e', d' - e') \mid d'e' = \tfrac{n}{4},\ d' > e' > 0\right\}.$$

The remainder of the proof is the same as for n odd. □

Pell's equation. Let $d \in \mathbb{N}$ be squarefree, and consider

$$x^2 - y^2 d = \begin{cases} \pm 1 & \text{if} \quad d \underset{(4)}{\equiv} 2, 3 \\ \pm 4 & \text{if} \quad d \underset{(4)}{\equiv} 1. \end{cases} \tag{32}$$

This equation is closely related to the quadratic number field $K = \mathbb{Q}[\sqrt{d}]$ with ring of integers[2]

$$\mathcal{O}_K := \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if} \quad d \underset{(4)}{\equiv} 2, 3 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if} \quad d \underset{(4)}{\equiv} 1. \end{cases}$$

The *units* $\mathcal{O}_K^* \subset \mathcal{O}_K$ are simply the elements which are invertible in $\mathcal{O}_K$. We claim the following:

THEOREM 163. *For $d \underset{(4)}{\equiv} 2, 3$ (resp. 1), the units $\mathcal{O}_K^*$ are exactly the numbers $x + y\sqrt{d}$ (resp. $\frac{x+y\sqrt{d}}{2}$) such that x, y are integers satisfying Pell's equation* (32)*.*

PROOF. Assume $d \underset{(4)}{\equiv} 2, 3$, so that the left-hand side of (32) is the norm $N_K(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d})$ for $K = \mathbb{Q}[\sqrt{d}]$. We may view the norm as a homomorphism

$$N_K : \mathcal{O}_K \backslash \{0\} \to \mathbb{Z} \backslash \{0\}$$

of multiplicative monoids (i.e. $N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$).

[2]The notation $\mathbb{Z}[\mu]$ (resp. $\mathbb{Q}[\mu]$) means in general the ring of polynomials in μ with integer (resp. rational) coefficients, but here α satisfies a quadratic equation $\mu^2 = d$ or $\mu^2 = \mu + b$ ($b \in \mathbb{Z}$ resp. $\mathbb{Q}$), so every "polynomial" is equal to a unique expression of the form $a + b\mu$, with $a, b \in \mathbb{Z}$ (resp. $\mathbb{Q}$). That is, for our purposes here, $\mathbb{Z}[\mu] = \{a + b\mu \mid a, b \in \mathbb{Z}\}$.

If $\alpha = x + y\sqrt{d} \in \mathcal{O}_K^*$, then there exists $\beta \in \mathcal{O}_K$ with $\alpha\beta = 1$

$$\implies 1 = N_K(1) = N_K(\alpha\beta) = N_K(\alpha)N_K(\beta)$$

with both $N_K(\alpha), N_K(\beta) \in \mathbb{Z}$. Hence $N_K(\alpha) = \pm 1$ and (x, y) satisfies Pell.

Conversely, if $N_K(\alpha) = \pm 1$ for some $\alpha = x + y\sqrt{d} \in \mathcal{O}_K$, then (writing $\tilde{\alpha} = x - y\sqrt{d}$) $\alpha\tilde{\alpha} = \pm 1 \implies \alpha(\pm\tilde{\alpha}) = 1 \implies \alpha$ invertible in $\mathcal{O}_K \implies \alpha \in \mathcal{O}_K^*$.

For the case $d \underset{(4)}{\equiv} 1$, one just has to write $\alpha = \frac{x+y\sqrt{d}}{2}$ so that $4N_K(\alpha) = x^2 - y^2 d$, and Pell again is equivalent to $N_K(\alpha) = \pm 1$. □

Powers of units are units, and it turns out that there exists a "fundamental unit" $u = x_1 + y_1\sqrt{d}$ (to be proved in §IV.C) such that

$$\mathcal{O}_K^* = \left\{ \pm u^\ell \mid \ell \in \mathbb{Z} \right\}.$$

Let's apply this to $d = 5$, for which $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and

$$\varphi = \frac{1+\sqrt{5}}{2}$$

— the golden ratio, which satisfies $1 + \varphi = \varphi^2$ — is our u. Writing as above $\widetilde{x + y\sqrt{d}} := x - y\sqrt{d}$, and defining $(x_n, y_n) \in \mathbb{Z}^2$ by

$$\varphi^n = \frac{x_n + y_n\sqrt{d}}{2},$$

we have

$$x_n = \varphi^n + \tilde{\varphi}^n, \quad y_n = \frac{\varphi^n - \tilde{\varphi}^n}{\sqrt{5}}.$$

Since each $\varphi^n \in \mathcal{O}_K^*$, by Theorem 163 each (x_n, y_n) solves the equation

$$x^2 - 5y^2 = \pm 4. \tag{33}$$

Now $y_0 = 0$, $y_1 = 1$, and (using $1 + \varphi = \varphi^2$, $1 + \tilde{\varphi} = \tilde{\varphi}^2$)

$$\begin{aligned} y_{n-2} + y_{n-1} &= \frac{\varphi^{n-2} - \tilde{\varphi}^{n-2} + \varphi^{n-1} - \tilde{\varphi}^{n-1}}{\sqrt{5}} \\ &= \frac{\varphi^{n-2}(1+\varphi) - \tilde{\varphi}^{n-2}(1+\tilde{\varphi})}{\sqrt{5}} \\ &= \frac{\varphi^n - \tilde{\varphi}^n}{\sqrt{5}} \\ &= y_n. \end{aligned}$$

Therefore the $\{y_n\}$ are the **Fibonacci numbers**, and the $(\pm x_n, \pm y_n)$ give the complete solutions of (32), which is not just a set but a group (namely $\mathcal{O}^*_{\mathbb{Q}[\sqrt{5}]}$) of the form [i.e. isomorphic to] $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$.

CHAPTER 20

Units in quadratic number rings

Let $d \in \mathbb{Z}$ be non-square, $K = \mathbb{Q}(\sqrt{d})$. (That is, $d = e^2 f$ with f squarefree, and $K = \mathbb{Q}(\sqrt{f})$.) For $\alpha = a + b\sqrt{d} \in K$, $N_K(\alpha) = \alpha\tilde{\alpha} = a^2 - b^2 d \in \mathbb{Q}$. If $d \underset{(4)}{\equiv} 1$, take $S := \mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$; otherwise take $S := \mathbb{Z}[\sqrt{d}]$. This is a bit more general than the setting of §IV.B: in the cases *(i)* d not squarefree or *(ii)* $d \underset{(4)}{\equiv} 1$ and $S = \mathbb{Z}[\sqrt{d}]$, S will be a *proper* subring of $\mathcal{O}_K$. (We will still call S "a ring of integers in K", just not "the" ring of integers, which is $\mathcal{O}_K$.) The idea is that this extra generality might allow one to treat some extra Diophantine equations.

Clearly the norm N_K takes integer values on S, since $S \subset \mathcal{O}_K$. If for $\alpha \in S$, $N_K(\alpha) = \pm 1$, then $\alpha^{-1} = N_K(\alpha) \cdot \tilde{\alpha} \in S$. Conversely, if $\alpha, \alpha^{-1} \in S$ then $N_K(\alpha)N_K(\alpha^{-1}) = N_K(\alpha\alpha^{-1}) = N_K(1) = 1$ forces $N(\alpha) = \pm 1$ (since both $N(\alpha)$, $N(\alpha^{-1})$ must be integers). So the units

$$S^* = \{\alpha \in S \mid N_K(\alpha) = \pm 1\}.$$

The quadratic imaginary case. The following result sums it up: the units are just the (exceedingly few) roots of unity.

PROPOSITION 164. *Let $d < 0$, with S as above. Then $S^* = \{\pm 1\}$ unless:*
• *$d = -1$ and $S = \mathbb{Z}[\sqrt{-1}]$ ($\implies S^* = \{\pm 1, \pm i\}$); or*
• *$d = -3$ and $S = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ ($\implies S^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$).*

PROOF. CASE 1 ($S = \mathbb{Z}[\sqrt{d}]$): The solutions to Pell's equation

$$1 = N_K(x + y\sqrt{d}) = x^2 + y^2|d|$$

are $(\pm 1, 0)$ and, if $d = -1$, $(0, \pm 1)$.

CASE 2 ($d \underset{(4)}{\equiv} 1, S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$): We have to solve $\pm 1 = N_K(\frac{x+y\sqrt{d}}{2})$, or equivalently

$$4 = x^2 + y^2|d|.$$

The options are $(\pm 2, 0)$ and, if $d = -3$, $(\pm 1, \pm 1)$ (4 possibilities). □

The fundamental unit in a real quadratic ring of integers. In this case the units form an abelian group of rank[1] one:

THEOREM 165. *Let $d > 1$, and S be as above. Then S has a least unit $u > 1$, and $S^* = \{\pm u^r \mid r \in \mathbb{Z}\}$. That is, $\{\alpha \in S^* \mid \alpha > 1\}$ is nonempty and has a least element; and together with -1, the element generates S^*.*

DEFINITION 166. The element $u \in S^*$ in Theorem 165 is called a **fundamental unit** for S (or for K, if $S = \mathcal{O}_K$).

EXAMPLE 167 ($S = \mathcal{O}_K$).
- $d = 3 \implies u = 2 + \sqrt{3}$
- $d = 94 \implies u = 2143295 + 221064\sqrt{94}$
- $d = 95 \implies u = 39 + 4\sqrt{95}$

REMARK 168. These results (the Theorem and Proposition above) have a beautiful generalization due to Dirichlet: *any algebraic number field* (fields which are also finite dimensional vector spaces over $\mathbb{Q}$) *K has $n = \dim_{\mathbb{Q}} K$ distinct embeddings in the complex numbers $\mathbb{C}$*, which may further be subdivided into r_1 embeddings in $\mathbb{R}$ and r_2 complex-conjugate pairs of complex embeddings, with $r_1 + 2r_2 = n$. Dirichlet's **Theorem on Units** says that if $\mathcal{O}_K := K \cap \bar{\mathbb{Z}}$ denotes the numbers solving a monic polynomial equation with integer coefficients, then

$$\mathcal{O}_K^* \cong \mathbb{Z}^{r_1+r_2-1} \times \{\text{roots of 1 in } K\}.$$

Proposition 164 corresponds to the case $r_1 = 0$, $r_2 = 1$, while Theorem 165 corresponds to the case $r_1 = 2$, $r_2 = 0$.

[1] Any finitely generated abelian group is of the form $G \cong \mathbb{Z}^r \times \{\text{finite abelian group}\}$. The rank of G is defined to be r.

Now let $n \in \mathbb{N}$, and take m to be the nearest integer to $n\sqrt{d}$, so that $\frac{m}{n}$ is the best approximation to $\sqrt{d}$ with denominator n; in particular,

$$|m - n\sqrt{d}| < \tfrac{1}{2} \implies \left|\frac{m}{n} - \sqrt{d}\right| < \frac{1}{2n}. \tag{34}$$

If we "know something" about $\sqrt{d}$, we should be able to get a better approximation (relative to the denominator)[2] than (34). So assuming $S^* \backslash \{\pm 1\}$ is nonempty, let $\alpha = a + b\sqrt{d} \in S^*$ with $a, b > 0$. (One of $\pm\alpha_0, \pm\tilde{\alpha}_0$ has this form for any $\alpha_0 \in S^* \backslash \{\pm 1\}$.) We find

$$|b\sqrt{d} - a| = |\tilde{\alpha}| = \frac{1}{|\alpha|} = \frac{1}{\alpha} = \frac{1}{a + b\sqrt{d}} < \frac{1}{b\sqrt{d}} < \frac{1}{b},$$

which indeed yields an approximation

$$\left|\sqrt{d} - \frac{a}{b}\right| < \frac{1}{b^2\sqrt{d}}$$

improving (34). This motivates

DEFINITION 169. We will call

$$A := \{\alpha = a + b\sqrt{d} \in S \mid a, b \in \mathbb{N}, \underbrace{|\tilde{\alpha}| < \tfrac{1}{b}}_{(*)}\}$$

the set of "well-approximable" elements of S.

REMARK 170. To illustrate the terminology, I note that in $|2a - \alpha| = |\tilde{\alpha}| < \frac{1}{b}$, one may regard $2a$ as an approximation to α. But one can do much better: $(*)$ actually ensures that

$$2a - \cfrac{a^2 - b^2 d}{2a - \cfrac{a^2 - b^2 d}{2a - \cfrac{a^2 - b^2 d}{\cdots}}}$$

converges rapidly to α. The resulting connection between solutions of Pell's equation and continued fractions was of great historical importance in the development of Diophantine analysis.

Our argument above shows that about a quarter of S^* lies in A; what we really want to do is go in the opposite direction: show how

[2] but (necessarily) with a different denominator

to get a unit "out of" A, which first involves showing A is "big" and bounding norms of its elements.

LEMMA 171. $|A| = \infty$.

PROOF. Suppose otherwise: then there exists $n \in \mathbb{N}$ such that

$$\frac{1}{n} < |\tilde{\alpha}| \ \ (\forall \alpha \in A). \tag{35}$$

Since the $n+1$ numbers

$$\lambda_r := r\sqrt{d} - \lfloor r\sqrt{d} \rfloor, \ \ r = 0, 1, \ldots, n$$

lie in $[0,1) = \cup_{i=1}^{n} [\frac{i-1}{n}, \frac{i}{n})$, two must lie in the same subinterval:

$$\frac{1}{n} > |\lambda_s - \lambda_t| = \left| (\lfloor t\sqrt{d} \rfloor - \lfloor s\sqrt{d} \rfloor) - (t-s)\sqrt{d} \right| =: |a - b\sqrt{d}|,$$

where we may assume $t > s$ so that $a, b > 0$. Hence,

$$\frac{1}{b} \geq \frac{1}{n} > |a - b\sqrt{d}| =: |\tilde{\alpha}|$$

and α belongs to A, contradicting (35). □

LEMMA 172. $\alpha \in A \implies |N(\alpha)| < 1 + 2\sqrt{d}$.

PROOF. Write $\alpha = a + b\sqrt{d} = \tilde{\alpha} + 2b\sqrt{d}$. Then $\alpha \in A$ implies $|\tilde{\alpha}| < \frac{1}{b}$ and $a, b > 0$, so that

$$|N(\alpha)| = \alpha \cdot |\tilde{\alpha}| < \left(\tfrac{1}{b} + 2b\sqrt{d} \right) \cdot \tfrac{1}{b} = \tfrac{1}{b^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

□

LEMMA 173. *There exist elements $\alpha = a + b\sqrt{d}$ and $\alpha' = a' + b'\sqrt{d}$ of A such that*
(i) $\alpha > \alpha' > 0$,
(ii) $|N(\alpha)| = |N(\alpha')| = n$, and
(iii) $a \underset{(n)}{\equiv} a'$, $b \underset{(n)}{\equiv} b'$.

PROOF. Set

$$A_{n,r,s} := \{\alpha \in A \mid |N(\alpha| = n, \ a \underset{(n)}{\equiv} r, \ b \underset{(n)}{\equiv} s\}$$

for each of the *finitely many* integer 3-tuples (n, r, s) with

$$1 \leq n < 1 + 2\sqrt{d}, \;\; r \in \{0, 1, \ldots, n-1\}, \;\; s \in \{0, 1, \ldots, n-1\}.$$

By Lemma 172, each $\alpha \in A$ lies in one of these. Since (by Lemma 171) $|A| = \infty$, some $A_{n,r,s}$ contains more then one element. (Note that $\alpha' = a' + b'\sqrt{d} > 0$ because $a', b' \in \mathbb{N}$.) □

We are now prepared for the first big step toward Theorem 165:

PROPOSITION 174. *There exists $v \in \mathbb{Z}[\sqrt{d}]^*$ such that $v > 1$.*

PROOF. With $\alpha = a + \sqrt{d}$ and $\alpha' = a' + b'\sqrt{d}$ as in Lemma 173, set $v := \frac{\alpha}{\alpha'} \in \mathbb{Q}(\sqrt{d})$ and $\gamma := \frac{a-a'}{n} + \frac{b-b'}{n}\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. We evidently have $\alpha = \alpha' + n\gamma$, which together with $n = |N(\alpha')| = \pm\alpha'\tilde{\alpha}'$ yields

$$v = 1 + \frac{n\gamma}{\alpha'} = 1 \pm \tilde{\alpha}'\gamma \in \mathbb{Z}[\sqrt{d}].$$

Finally, since $\pm N(\alpha) = n = \pm N(\alpha')$,

$$N(v) = \frac{N(\alpha)}{N(\alpha')} = \pm 1,$$

and $\alpha > \alpha' > 0 \implies v > 1$. □

LEMMA 175. *For $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$,*

$$a, b > 0 \iff \alpha > \sqrt{|N(\alpha)|}.$$

PROOF. We have

$$\begin{aligned}
\alpha > \sqrt{|N(\alpha)|} &\iff \alpha^2 > |N(\alpha)| \text{ and } \alpha > 0 \\
&\iff \alpha^2 > \alpha|\tilde{\alpha}| > 0 \\
&\iff \alpha > |\tilde{\alpha}| \\
&\iff \alpha > \pm\tilde{\alpha} \\
&\iff a, b > 0,
\end{aligned}$$

since $a = \frac{\alpha+\tilde{\alpha}}{2}$ and $b = \frac{\alpha-\tilde{\alpha}}{2\sqrt{d}}$. □

At last we are ready for the

PROOF OF THEOREM 165. With v as in Proposition 174, set

$$U_v := \{\alpha \in S^* \mid 1 < \alpha \leq v\},$$

which is nonempty (as it contains v). Now writing $\alpha = \frac{a+b\sqrt{d}}{2}$ (so as to include the case $S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$), we have by Lemma 173

$$\begin{aligned} \alpha \in U_v &\implies v \geq \alpha > 1 = \sqrt{|N(\alpha)|} \\ &\implies a, b > 0 \text{ and } \alpha \leq v \\ &\implies \frac{a}{2}, \frac{b}{2} < v. \end{aligned}$$

So the cardinality $|U_v| \leq (2v)^2 < \infty$, and U_v therefore has a least element u, which is then also the least element of $\{\alpha \in S^* \mid 1 < \alpha\}$ (i.e. a fundamental unit).

Clearly S^* contains $\{\pm u^m \mid m \in \mathbb{Z}\}$. To show the reverse inclusion, let $x \in S^*$. Then $|x| = \pm x \in S^*$, and there exists an $r \in \mathbb{Z}$ such that $u^r < |x| \leq u^{r+1}$ (indeed, $r = \lfloor \frac{\log |x|}{\log u} \rfloor$). Multiplying by u^{-r} yields $1 < |x|u^{-r} \leq u$, with $|x|u^{-r} \in S^*$. But by "leastness" of u, we must then have $|x|u^{-r} = u$, hence $|x| = u^{r+1}$ and $x = \pm u^{r+1}$. □

Computing the fundamental unit. Recall that $d \in \mathbb{N}$ is nonsquare, and $S := \mathbb{Z}[\sqrt{d}]$ or (only in case $d \underset{(4)}{\equiv} 1$) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$; we have $S \subseteq \mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{d})$.

THEOREM 176. *For $S = \mathbb{Z}[\sqrt{d}]$ (resp. $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$), let $a, b \in \mathbb{N}$ give a solution of $a - db^2 = \pm 1$ (resp. $a^2 - db^2 = \pm 4$), with b least possible. Then $a + b\sqrt{d}$ (resp. $\frac{a+b\sqrt{d}}{2}$) is a fundamental unit of S.*

PROOF. (I will do the case $S = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$; the other one is similar.)

Let $d = 5$; the solution of $a^2 - 5b^2 = \pm 4$ with least possible $b \in \mathbb{N}$ is $(a, b) = (1, 1)$, so set $u := \frac{1+\sqrt{5}}{2}$. Now any $w \in S$ is of the form $\frac{s+t\sqrt{5}}{2}$, $s, t \in \mathbb{Z}$; and $1 < w \in S^* \implies N(w) = \pm 1$ (and $w > 1$) $\implies w > \sqrt{|N(w)|}$, which by Lemma 173 $\implies s, t > 0 \implies s, t \geq 1 \implies w \geq u$. So u is the fundamental unit (= least element of $\{\alpha \in S^* \mid \alpha > 1\}$, by Theorem 165).

Next let $d \neq 5$ (i.e. $d > 5$ with $d \underset{(4)}{\equiv} 1$), and take $v := \frac{m+n\sqrt{d}}{2}$ (with $m, n \in \mathbb{Z}$) to be a fundamental unit of S. By definition we have $v > 1$, and so Lemma 173 $\implies m, n > 0$. Now

$$\pm 4 = N(2) \cdot N(v) = N(2v) = N(m + n\sqrt{d}) = m^2 - n^2 d.$$

So we have two solutions (in $\mathbb{N} \times \mathbb{N}$) to $x^2 - dy^2 = \pm 4$: (m, n) and (a, b). As the second of these has b least possible, $n \geq b$. Put $w := \frac{a+b\sqrt{d}}{2}$.

I claim that w belongs to $\{\alpha \in S^* \mid \alpha > 1\}$. Indeed, reducing $a^2 - db^2 = \pm 4$ modulo 2 gives $a^2 - b^2 \underset{(2)}{\equiv} 0 \implies a \underset{(2)}{\equiv} b \implies w \in S$; and $N(w) = \frac{a^2 - b^2 d}{4} = \pm 1 \implies w \in S^*$; finally, $a, b \in \mathbb{N} \implies w > 1$. So the claim holds, and since v is least in $\{\alpha \in S^* \mid \alpha > 1\}$, $v \leq w$. In fact, by Theorem 165 (regarding structure of S^*), we must have $w = v^r$ for some $r \in \mathbb{N}$.

It now suffices to show that $r = 1$. Suppose instead that $r > 1$: then writing out $w = v^r$ as

$$\frac{a + b\sqrt{d}}{2} = \left(\frac{m + n\sqrt{d}}{2}\right)^r = \frac{m^r + \binom{r}{1} n\sqrt{d} m^{r-1} + \cdots}{2^r}$$

and comparing coefficients of $\sqrt{d}$ yields

$$\frac{b}{2} = \frac{rnm^{r-1}}{2^r} + \cdots \geq \frac{rnm^{r-1}}{2^r}.$$

Since $n \geq b$, multiplying through by 2^r gives

$$2^{r-1} b \geq rnm^{r-1} \geq rbm^{r-1}$$

hence (using $r > 1$)

$$2^{r-1} \geq rm^{r-1} > m^{r-1},$$

which forces $m = 1$. So the Pell equation becomes

$$1^2 - n^2 d = \pm 4 (= -4) \quad \implies \quad n^2 d = 1 + 4 = 5,$$

which is a contradiction as $d > 5$.

Therefore $r = 1$ and the minimal-b-solution w equals the fundamental unit v, as desired. □

Exercises

(1) Find the fundamental units of $\mathbb{Q}(\sqrt{d})$ (that is, of its ring of integers) for $d = 7$, 30, and 53.
(2) Use a unit in $\mathbb{Z}[\sqrt{30}]$ to prove that the difference between $241/44$ and $\sqrt{30}$ is less that 5×10^{-5}.
(3) Let $n \in \mathbb{Z}$, $n > 2$ and put $d = n^2 - 2$. Show that $n^2 - 1 + n\sqrt{d}$ is a unit of $\mathbb{Z}[\sqrt{d}]$. Is it necessarily the fundamental unit? (Give a proof or a counterexample.)

CHAPTER 21

Pell's equation and related problems

Let $d \in \mathbb{Z}$ be non-square, $K = \mathbb{Q}(\sqrt{d})$. As usual, we take $S := \mathbb{Z}[\sqrt{d}]$ (for any d) or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ (only if $d \underset{(4)}{\equiv} 1$). We have proved that

- S has a least ("fundamental") unit $u > 1$, and $S^* = \{\pm u^r \mid r \in \mathbb{Z}\}$,
- $u = a + b\sqrt{d}$ (resp. $\frac{a+b\sqrt{d}}{2}$) where (a, b) is the positive-integral solution of $x^2 - y^2 d = \pm 1$ (resp. ± 4) with b as small as possible,

and promised some examples. Here they are:

EXAMPLE 177 ($S = \mathbb{Z}[\sqrt{2}]$). $(a, b) = (1, 1)$ yields the minimal-b solution (in $\mathbb{N} \times \mathbb{N}$) to $a^2 - 2b^2 = \pm 1$; so $u = 1 + \sqrt{2}$ is the fundamental unit.

EXAMPLE 178 ($S = \mathbb{Z}[\sqrt{20}]$). Notice that $a^2 - 20b^2 = \pm 1$ is equivalent to "$20b^2 \pm 1$ is a square". So we make a table

$b =$	1	2	$\cdots$
$20b^2 + 1 =$	21	$\boxed{81}$	$\cdots$
$20b^2 - 1 =$	19	79	$\cdots$

in which (from left to right) the first square to appear is $81 = a^2$, $a = 9$. So a minimal-b solution is $(a, b) = (9, 2)$, and the fundamental unit is $u = 9 + 2\sqrt{20}$.

EXAMPLE 179 ($S = \mathbb{Z}[\sqrt{14}]$). To solve $a^2 - 14b^2 = \pm 1$, we again make a table:

$b =$	1	2	3	4	$\cdots$
$14b^2 + 1 =$	15	57	127	$\boxed{225} = 15^2$	$\cdots$
$14b^2 - 1 =$	13	55	125	223	$\cdots$

and conclude that $u = 15 + 4\sqrt{14}$.

EXAMPLE 180 ($S = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$). Look at $a^2 - 17b^2 = \pm 4$, and

$b =$	1	2	$\cdots$
$17b^2 + 4 =$	21	72	$\cdots$
$17b^2 - 4 =$	13	$\boxed{64}$	$\cdots$

$\implies u = \frac{8+2\sqrt{17}}{2} = 4 + \sqrt{17}$.

Of course, you won't be able to do them all by hand:

EXAMPLE 181 ($S = \mathbb{Z}[\sqrt{46}]$). $u = 24335 + 3588\sqrt{46}$.

But obviously the algorithm we have been using could be set up vey easily in PARI.

Apparently the integral solutions of Pell's equation

$$x^2 - dy^2 = \pm 1 \quad (d \in \mathbb{N} \text{ nonsquare}) \tag{36}$$

had been studied with partial success in medieval India, and before that by Diophantus himself. *We* know that they are in 1-1 correspondence with the units $\mathbb{Z}[\sqrt{d}]^*$ (via $x + y\sqrt{d}$), and that the same goes (via $\frac{x+y\sqrt{d}}{2}$) for solutions of

$$x^2 - dy^2 = \pm 4 \quad (d \in \mathbb{N} \text{ nonsquare}, d \underset{(4)}{\equiv} 1) \tag{37}$$

and $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]^*$. We can therefore find all solutions to (36)-(37) by computing a fundamental unit u and taking $\pm u^r$ ($r \in \mathbb{Z}$). If $u = x_1 + y_1\sqrt{d}$, then setting

$$u^r =: x_r + y_r\sqrt{d},$$

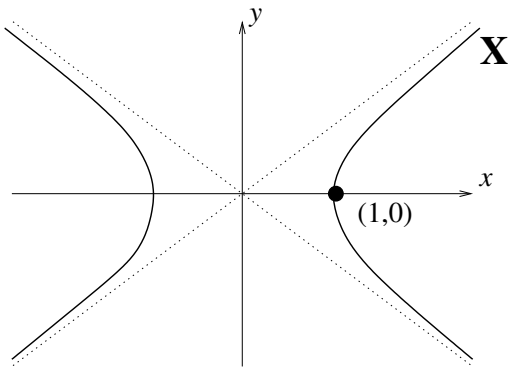
we have $\tilde{u}^r = x_r - y_r\sqrt{d}$ and

$$x_r = \frac{u^r + \tilde{u}^r}{2}\ ,\ \ y_r = \frac{u^r - \tilde{u}^r}{2\sqrt{d}}. \tag{38}$$

Now suppose for simplicity that (x_1, y_1) satisfies

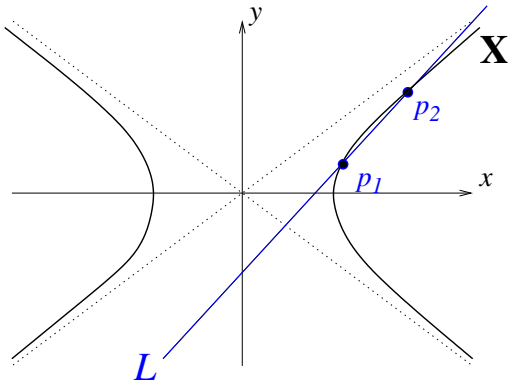
$$X^2 - dY^2 = +1. \tag{39}$$

We would like to geometrically interpret multiplication in $\mathbb{Z}[\sqrt{d}]^*$ on the hyperbola $\mathbf{X}$



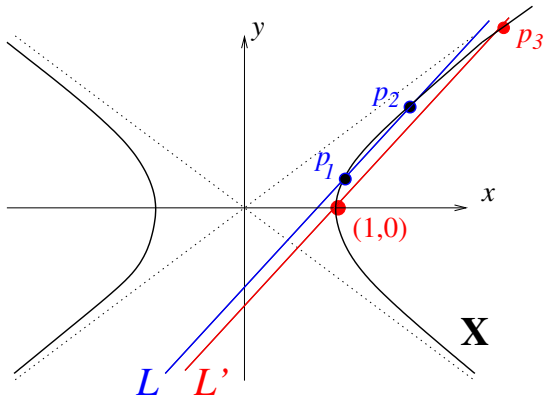
comprising solutions of (39), so as to view our correspondence between units and solutions as a homomorphism (in fact, isomorphism) of groups. That is, we want a *group law*[1] on the points of $\mathbf{X}$ (and for the integer points to be *closed* under this binary operation).

Given points p_1 and p_2 on $\mathbf{X}$, draw the line $L = L_{p_1p_2}$:



[1]This is another standard term for "binary operation satisfying the group axioms".

(If $p_1 = p_2$, then L is the line *tangent* to $\mathbf{X}$ at this point.) Next, parallel-translate this line until it goes through $(1,0)$ and one other point p_3,



and call the result L'. Finally, set

$$p_1 * p_2 := p_3;$$

$(1,0)$ is clearly the identity element in this (evidently abelian) group.[2] But wait: we have not checked existence of inverses, or closure, or associativity! So how do we know the integer points of $\mathbf{X}$, written $\mathbf{X}(\mathbb{Z})$, constitute a group? The following will take care of that:

THEOREM 182. *The map*

$$\varphi : \mathbb{Z}[\sqrt{d}]^* \to \mathbf{X}(\mathbb{Z})$$

sending $x + y\sqrt{d} \mapsto (x,y)$, *identifies "$\cdot$" (multiplication) on the left-hand side with "$*$" on the right-hand side, and is 1-to-1 and onto. Hence* $(\mathbf{X}(\mathbb{Z}), *)$ *is a group, and* φ *is an isomorphism of groups.*

PROOF. It is easy to see that φ is a bijection: if $x + y\sqrt{d}, x' + y'\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^*$ have $(x,y) = (x',y')$, then obviously they're equal. So φ is 1-1. Moreover, if $(x,y) \in \mathbf{X}(\mathbb{Z})$, then $(x,y) \in \mathbb{Z}^2$ and $N(x + y\sqrt{d}) = x^2 - dy^2 = +1 \implies x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^*$, and φ is onto.

Now comes the work: to compute $p_1 * p_2 = (x,y) * (z,w)$, observe that L has slope $\frac{w-y}{z-x}$, so that $L' = \{(X,Y) \mid X = 1 + \frac{z-x}{w-y}Y\}$. To

[2]For those of you with some exposure to algebraic geometry, this is the group law on the *singular cubic* obtained by adding the "line at infinity" in $\mathbb{P}^2$ to the projective closure of the conic $\mathbf{X}$.

find $p_3 \in L' \cap \mathbf{X}$:

$$\left(1 + \tfrac{z-x}{w-y}Y\right)^2 = dY^2 + 1$$

has nonzero solution

$$Y = \frac{2\frac{z-x}{w-y}}{d - \left(\frac{z-x}{w-y}\right)^2} = \frac{2(z-x)(w-y)}{d(w-y)^2 - (z-x)^2},$$

but this is not yet in a useful form. We need to use the fact that p_1 and p_2 lie on $\mathbf{X}$, i.e. that

$$z^2 = dw^2 + 1\ , \quad x^2 = dy^2 + 1. \tag{40}$$

Applying (40) repeatedly to the expression for Y gives

$$\begin{aligned} Y = \frac{(z-x)(w-y)}{zx - (dwy+1)} &= \frac{(zx+dwy+1)(z-x)(w-y)}{z^2x^2 - (dwy+1)^2} \\ = \frac{(zx+dwy+1)(z-x)(w-y)}{d(w-y)^2} &= \frac{(zx+dwy+1)(z-x)}{d(w-y)} \\ = \frac{d(w-y)(wx+zy)}{d(w-y)} &= wx + zy, \end{aligned}$$

where I have left some of the work for you. Similarly, using (40), one shows that

$$(w-y) + (z-x)(wx+zy) = (w-y)(xz+dyw)$$

hence

$$X = 1 + \frac{z-x}{w-y}Y = 1 + \frac{z-x}{w-y}(wx+zy) = xz + dyw.$$

(Note that this already proves directly that $\mathbf{X}(\mathbb{Z})$ is closed under $*$!)

The verification we are after is now simple:

$$\begin{aligned} \varphi\{(x+y\sqrt{d})\cdot(z+w\sqrt{d})\} &= \varphi\{(xz+dyw) + (wx+zy)\sqrt{d}\} \\ &= (xz+dyw, wx+zy) \\ &= (x,y) * (z,w) \\ &= \varphi(x+y\sqrt{d}) * \varphi(z+w\sqrt{d}), \end{aligned}$$

which (together with φ being bijective) identifies "$\cdot$" with "$*$". Hence $(\mathbb{Z}[\sqrt{d}]^*, \cdot)$ is a group $\implies$ $(\mathbf{X}(\mathbb{Z}), *)$ is a group. With this established, we also see that φ is a homomorphism, hence an isomorphism. $\square$

Now to the business of solving equations. We will use the notation $\varphi(x + y\sqrt{d}) := (x, y)$ more broadly than in the specific (group-homomorphism) context above.

EXAMPLE 183. Suppose we wish to find *all integer solutions* of $x^2 - 2y^2 = 1$. The fundamental unit of $S = \mathbb{Z}[\sqrt{2}]$ is $u = 1 + \sqrt{2}$, so $S^* = \{\pm u^m \mid m \in \mathbb{Z}\}$ gives all solutions of $N(\cdot) = \pm 1$. Since $N(u) = 1^2 - 2 \cdot 1^2 = -1$, $\{\pm u^{2m} \mid m \in \mathbb{Z}\}$ gives all solutions to $N(\cdot) = 1$; that is,

$$\varphi(\pm u^{2m}) =: \pm(x_m, y_m), \quad m \in \mathbb{Z}$$

yields all solutions to the equation.

As in (38),

$$x_m = \frac{u^{2m} + \tilde{u}^{2m}}{2} \text{ and } y_m = \frac{u^{2m} - \tilde{u}^{2m}}{2\sqrt{2}};$$

computing $u^2 = 3 + 2\sqrt{2}$ gives

$$x_m = \frac{(3 + 2\sqrt{2})^m + (3 - 2\sqrt{2})^m}{2} \text{ and } y_m = \frac{(3 + 2\sqrt{2})^m - (3 - 2\sqrt{2})^m}{2\sqrt{2}}.$$

EXAMPLE 184. Consider the equation $x^2 - 5y^2 = 1$. We take $S = \mathbb{Z}[\sqrt{5}]$ (even though $5 \underset{(4)}{\equiv} 1$), for which $u = 2 + \sqrt{5}$, with $N(u) = 2^2 - 5 \cdot 1^2 = -1$. Noting that $u^2 = 9 + 4\sqrt{5}$, the complete list of integral solutions is $\{\varphi(\pm u^{2m})\} =$

$$\left\{ \pm \left(\tfrac{(9+4\sqrt{5})^m + (9-4\sqrt{5})^m}{2}, \tfrac{(9+4\sqrt{5})^m - (9-4\sqrt{5})^m}{2\sqrt{5}} \right) \right\}.$$

Exercises

(1) Give formulae for all the solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ (if any) to $x^2 - 6y^2 = 1$.

(2) Give formulae for all the solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ (if any) to $9x^2 - 7y^2 = 1$.

CHAPTER 22

Unique factorization in number rings

What can this possibly have to do with solving Diophantine equations?! You're about to find out! Let's start by reviewing the formalism for solving Pell's equation problems.

EXAMPLE 185. The equation

$$x^2 - 75y^2 = 1$$

can be thought of (since $75 = 5^2 3$) as saying "the number $x + 5\sqrt{3}y$ has norm 1". So we need to find the units (elements of norm ± 1) in $S = \mathbb{Z}[5\sqrt{3}] \subset \mathbb{Q}(\sqrt{3})$ and pick out those of norm $+1$. To determine the units, we have to find the fundamental unit u of S. There are two ways to do this. Either (A) use the table

$b =$	1	2	3	$\cdots$
$75b^2 + 1 =$	76	301	$\boxed{676} = 26^2$	$\cdots$
$75b^2 - 1 =$	74	299	674	$\cdots$

or (B) use the facts that $\mathbb{Z}[5\sqrt{3}]^* \subset \mathbb{Z}[\sqrt{3}]^*$ and that the fundamental unit of $\mathbb{Z}[\sqrt{3}]$ is $v = 2 + \sqrt{3}$ (easier to find), so that u is the first power (namely v^3) of v lying in $\mathbb{Z}[5\sqrt{3}]$. Both (A) and (B) give $u = 26 + (5\sqrt{3})3 = 26 + 15\sqrt{3}$, and $N(u) = 676 - 225 \cdot 3 = 1 \implies \{\varphi(\pm u^m)\}$ is the complete list of solutions.[1]

EXAMPLE 186. What if we are presented with an equation such as

$$x^2 - 14y^2 = 5?$$

This isn't of "Pell-equation type".

[1] Recall that here $\varphi(x + y\sqrt{d})$ just means (x, y).

Let's set $S = \mathbb{Z}[\sqrt{14}]$ and see how far we can get. First, $u = 15 + 4\sqrt{14}$ from Example IV.D.3, and $N(u) = 1$. Now we note that

$$5 = -(3 + \sqrt{14})(3 - \sqrt{14})$$

in S. Given $\alpha = x + y\sqrt{14} \in S$ with $N(\alpha) = 5$, we have

$$\alpha\tilde{\alpha} = 5 \implies \alpha \mid 5 = -\beta\tilde{\beta} \text{ in } S.$$

Suppose we could conclude from this that $\alpha \mid \beta$ or $\alpha \mid \tilde{\beta}$ — after all, α has *prime norm* so itself is "irreducible" in the sense that any factorization $\alpha = rs$ (in S) must have $N(r) = 1$ or $N(s) = 1$ ($\implies$ r or s a unit). Since $\alpha, \beta, \tilde{\beta}$ all have norm ± 5, we would then have β/α or $\tilde{\beta}/\alpha$ a unit $\implies$

$$\alpha = \pm u^m \beta \text{ or } \pm u^m \tilde{\beta}.$$

Now reason that

$$N(\beta) = \beta\tilde{\beta} = -5$$

and so

$$N(\alpha) = N(\beta) \cdot N(\pm 1) \cdot N(u)^m = -5 \cdot 1 \cdot 1^m = -5,$$

rather than 5, a contradiction. So $x^2 - 14y^2 = 5$ *has no integer solutions*.

EXAMPLE 187. The last example can also be done by reducing modulo 7, but this one

$$x^2 - 14y^2 = -5$$

can't be. Because there *are* solutions, and we want *all* of them. (Greedy, innit?) Applying the same reasoning as above, we get $\alpha = \pm u^m \beta$ or $\pm u^m \tilde{\beta}$, and now there is no contradiction. The complete list of solutions is now simply

$$(x, y) = \left(\tfrac{\alpha+\tilde{\alpha}}{2}, \tfrac{\alpha-\tilde{\alpha}}{2\sqrt{14}}\right) = \begin{cases} \left(\pm\frac{u^m\beta+\tilde{u}^m\tilde{\beta}}{2}, \pm\frac{u^m\beta-\tilde{u}^m\tilde{\beta}}{2\sqrt{14}}\right) \\ \text{or } \left(\pm\frac{u^m\tilde{\beta}+\tilde{u}^m\beta}{2}, \pm\frac{u^m\tilde{\beta}-\tilde{u}^m\beta}{2\sqrt{14}}\right). \end{cases}$$

For instance, the top solution, with "+"-sign and $m = 0$ yields $(x, y) = (3, 1)$; and if $m = 1$, it gives $(x, , y) = (101, 27)$. Indeed, $101^2 - 14 \cdot 27^2 = 10201 - 10206 = -5$.

The property we are assuming for $S = \mathbb{Z}[\sqrt{14}]$ to make the leap

$$\alpha \mid \beta\tilde{\beta} \text{ and } \alpha \text{ irreducible} \implies \alpha \mid \beta \text{ or } \alpha \mid \tilde{\beta}$$

is called *unique factorization*, or to us, a "unique opportunity" to push our knowledge of rings a bit further!

DEFINITION 188. A domain (in this course) is a commutative ring R with the property $a, b \in R\backslash\{0\} \implies a \cdot b \in R\backslash\{0\}$.

As usual, the units (invertible elements) R^*form an (abelian) group.

DEFINITION 189. Two elements $a, b \in R$ are *associate* $\iff a = ub$ for some $u \in R^*$. (In this case we write $a \sim b$.)

(For example, we had $\alpha \sim \beta$ or $\alpha \sim \tilde{\beta}$ above.) As usual, we shall say that a *divides* b (and write $a \mid b$) when $b = ac$ for some $c \in R$. Note that

- $a \mid b$ and $b \mid a \iff a \sim b$,

since then $b = ac = bdc \implies (dc - 1)b = 0 \implies dc = 1$ (since R is a domain) $\implies c$ is a unit. Moreover,

- for $a, b \in R = \mathbb{Z}[\sqrt{d}]$ (or $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$), $a \mid b \implies N(a) \mid N(b)$. (Why?)

DEFINITION 190. (a) A nonzero $r \in R\backslash R^*$ is *irreducible* if the following property holds: $r = ab$ $(a, b \in R) \implies a \in R^*$ or $b \in R^*$.

(b) A nonzero $r \in R\backslash R^*$ is *prime* if the following property holds: $r \mid ab$ $(a, b \in R) \implies r \mid a$ or $r \mid b$.

In $\mathbb{Z}$, of course, primeness and irreducibility are the same thing.

EXAMPLE 191. In $R = \mathbb{Z}[\sqrt{-6}]$, let $\beta = 1 + 3\sqrt{-6}$; then we calculate

$$\beta\tilde{\beta} = (1 + 3\sqrt{-6})(1 - 3\sqrt{-6}) = 1 + 54 = 55 = 5 \cdot 11.$$

Suppose $\beta = ab$ in R. Then

$$N(a)N(b) = N(\beta) = \beta\tilde{\beta} = 55 \implies N(a) = 1, 5, 11, \text{ or } 55.$$

If $a = x + y\sqrt{-6}$ has norm 5 or 11, we have

$$x^2 + 6y^2 = 5 \text{ or } 11,$$

which is visibly impossible. Therefore $N(a) = 1$ and $N(b) = 55$ (or vice versa), and a (or b) is a unit! So β, and by similar reasoning $\tilde{\beta}$, 5, and 11, are all *irreducible* in R.

Now suppose 5 is *prime* in R. We would have $5 \mid \beta$ or $5 \mid \tilde{\beta}$, i.e. that $\frac{1 \pm 3\sqrt{-6}}{5}$ lies in R, which is clearly not true. So *irreducibility does not imply primeness in an arbitrary quadratic number ring*, and this is tied to nonuniqueness of factorization (or "failure of the fundamental theorem of arithmetic") in R.

On the other hand:

PROPOSITION 192. *In a domain R, $\pi \in R$ prime $\implies$ π irreducible.*

PROOF. Write $\pi = ab$. (We want to show that a or b belongs to R^*.) Now $\pi \mid ab$ and π prime imply that $\pi \mid a$ or $\pi \mid b$, say $\pi \mid a$. Then $a = \pi\rho \implies \pi = ab = (\pi\rho)b = \pi(\rho b) \implies \pi(\rho b - 1) = 0 \implies \rho b = 1$ (since $\pi \neq 0$ and R is a domain). Conclude that $b \in R^*$ as desired. □

So, *when* does the converse hold? (We hinted as much for $\mathbb{Z}[\sqrt{14}]$, after all.)

DEFINITION 193. A domain R is called a **UFD (unique factorization domain)** if every $r \in R \backslash \{0\}$ factors into a product of irreducible elements and the factorization is unique up to reodering and associates. (That is, if $x = up_1 \cdots p_r = vq_1 \cdots q_s$ with $u, v \in R^*$ and all p_i, q_i irreducible, then $r = s$ and $p_i \sim q_{\sigma(i)}$ $(\forall i)$ for some permutation $\sigma \in \mathcal{S}_r$.)

PROPOSITION 194. *In a UFD R, $\pi \in R$ irreducible $\implies$ π prime.*

PROOF. Let π be irreducible; in particular, $\pi \neq 0$ and $\pi \notin R^*$. Suppose that $\pi \mid ab$. We want to show that $\pi \mid a$ or $\pi \mid b$.

Decomposing a, b into irreducibles

$$a = p_1 \cdots p_\ell,\ b = p_{\ell+1} \cdots p_r \implies ab = p_1 \cdots p_r.$$

Now $\pi \mid ab \implies \pi\rho = ab$, $\rho = q_1 \cdots q_s$ (q_i irreducible) $\implies$ $\pi q_1 \cdots q_s = p_1 \cdots p_r$, and since R is a UFD, we conclude that $\pi \sim p_i$ for some i, hence that $\pi \mid a$ or b. □

EXAMPLE 195. $\mathbb{Z}$ and $\mathbb{Z}[\sqrt{14}]$ are UFDs, the former by the Fundamental Theorem of Arithmetic. I won't prove the latter now, but it justifies our examples above. $\mathbb{Z}[\sqrt{-6}]$ is not a UFD, as Example 191 demonstrates.

In order to treat one more example, we introduce the notion of *ideals* in a ring:

DEFINITION 196. An **ideal** I in a commutative ring R is a subgroup of $(R, +, 0)$ which is closed under multiplication by elements of R: that is, we have "$IR \subseteq I$". The **principal ideal** generated by $\alpha \in R$ is $(\alpha) := \{r\alpha \mid r \in R\}$. More generally, *the ideal generated by* $\alpha_1, \ldots, \alpha_s \in R$ is $(\alpha_1, \ldots, \alpha_s) = \{\alpha_1 r_1 + \cdots + \alpha_s r_s \mid r_1, \ldots, r_s \in R\}$. (You should check that these are closed under multiplication by R.)

It turns out that we can "take the quotient" R/I to get a new (commutative) ring with elements the group-cosets $r + I$. In particular, multiplication is well-defined since

$$(r + I)(s + I) = rs + rI + sI + I^2 = rs + I,$$

which would not work were I just a subring.

EXAMPLE 197. $\mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z}$. So these are familiar!

Here is an example of how to apply this to Diophantine equations:

EXAMPLE 198. Consider the equation

$$x^2 - 126y^2 = -5. \tag{41}$$

We first try to proceed in analogy to Examples 186-187: since $126 = 14 \cdot 3^2$, we use $S = \mathbb{Z}[3\sqrt{14}]$ in $\mathbb{Q}(\sqrt{14})$. The fundamental unit $u \in \mathbb{Z}[\sqrt{14}]^*$ is $15 + 4\sqrt{14}$, and $u_0 := u^2 = 449 + 120\sqrt{14}$ is the fundamental unit in S^*.

Write $5 = -\beta\tilde{\beta}$ as before. Given $\alpha \in S$ with $N(\alpha) = -5$, by the reasoning of Examples 186-187 we would like to conclude that

$$\alpha = \pm u_0^m \beta = \pm u^{2m} \beta$$

(or the same with $\tilde{\beta}$). Trouble is, this is wrong. The problem being that $\beta, \tilde{\beta}$ don't belong to S!!

Another approach is needed, and this is where an ideal comes in. Rewrite the equation (41) as $x^2 - 14(3y)^2 = -5$, or substituting $Y := 3y$,

$$x^2 - 14Y^2 = -5. \tag{42}$$

From Example 187, we have the solutions to this for $x, Y \in \mathbb{Z}$; now we just need to single out those solutions with

$$3 \mid Y.$$

This is equivalent to finding those α with $\alpha \equiv$ an integer in $\mathbb{Z}[\sqrt{14}]/(3)$. (Here (3) means the principal ideal generated by 3 in $\mathbb{Z}[\sqrt{14}]$.) We have $\beta \equiv \sqrt{14} \bmod (3)$, and $u^{\pm 1} \equiv \pm\sqrt{14} \bmod (3)$. So amongst the solutions $\alpha = \pm u^m \beta, \pm u^m \tilde{\beta}$ to (42), we want

$$\alpha = \pm u^{2m+1} \beta, \pm u^{2m+1} \tilde{\beta}$$

since modulo (3) these yield even powers of $\sqrt{14}$ (hence integers). The corresponding solutions to our original equation (41) are now

$$x = \frac{\alpha + \tilde{\alpha}}{2}, \quad y = \frac{1}{3} \cdot \frac{\alpha - \tilde{\alpha}}{2\sqrt{14}}.$$

As we shall see later, ideals are tied to the unique factorization property: for a number ring R,

$$\begin{aligned} R \text{ UFD} &\iff \text{irreducibles are prime in } R \\ &\iff \text{ideals are all principal in } R \\ &\iff \text{the group } Cl(R) := \frac{\text{ideals}}{\text{principal ideals}} \text{ is trivial.} \end{aligned}$$

The abelian group $Cl(R)$, which turns out to be finite for any number ring R, is called the **ideal class group** and has been a central object in algebraic number theory for well over a century.

CHAPTER 23

Elliptic curves

Turning to cubic (degree 3) equations, we shall begin with a geometric discussion which should make the number-theoretic aspects easier to visualize in the sections that follow.

Overview. For the purposes of this course, an **elliptic curve** will (almost) be the set of solutions to a "Weierstrass equation"

$$y^2 = x^3 + Ax + B \tag{43}$$

whose **discriminant** $4A^3 + 27B^2 \neq 0$. The "almost" means that *we have to add one more point o*, the "point at infinity", which is *postulated to be on every vertical line*. When speaking abstractly of this "curve" we shall denote it by E. When we want to refer to the solutions in a particular field $\mathbb{F}$, we shall denote that set by $E(\mathbb{F})$. Let $\mathbb{F} = \mathbb{C}$ for the moment.

You may wonder what "adding the point o" really means. It means that we are thinking in projective space

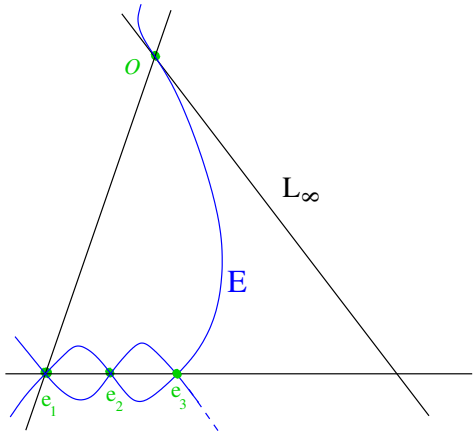
$$\begin{aligned}
\mathbb{P}^2(\mathbb{C}) &:= \Big(\mathbb{C}^3 \setminus \{0\}\Big) \Big/ (X,Y,Z) \underset{\forall \lambda \in \mathbb{C}^*}{\sim} (\lambda X, \lambda Y, \lambda Z) \\
&= \text{3-tuples } [X:Y:Z], \text{ with } X,Y,Z \text{ not all } 0, \text{ up to rescaling} \\
&= \text{lines through the origin in } \mathbb{C}^3 \\
&= \underset{[x:y:1]}{\mathbb{C}^2} \cup \underset{[x:y:0]}{\text{“line at } \infty\text{”}}
\end{aligned}$$

where the equation of E is

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Indeed, plugging in $[x : y : 1]$ gives back the original equation, whereas plugging in $[x : y : 0]$ gives $0 = x^3$, with the unique solution $[0 : 1 : 0] \in \mathbb{P}^2(\mathbb{C})$. (This is o.)

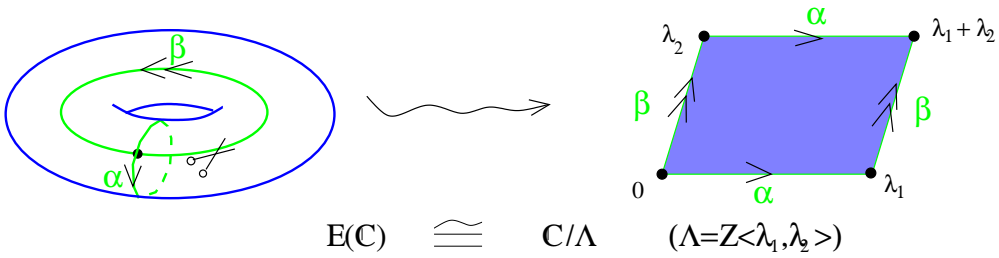
Schematically, we can draw the picture



where "e_i" means $(x, y) = (e_i, 0)$, and $e_1 + e_2 + e_3 = 0$, as can be seen from

$$x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3).$$

Topologically, $E(\mathbb{C})$ really takes the form of a torus[1]

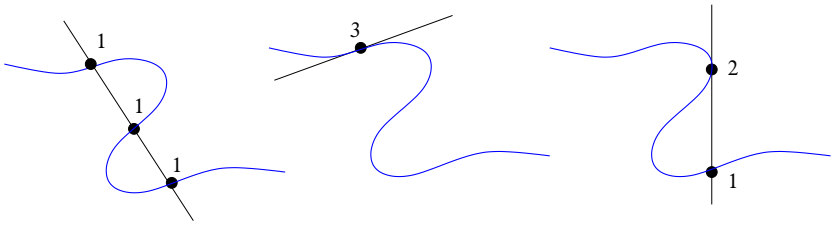


where the isomorphism is given by integration along the curve:

$$p \longmapsto \int_o^p \frac{dx}{y}.$$

(This takes the group structure we will define later to the obvious group structure on $\mathbb{C}/\Lambda$, Λ the lattice generated by $\lambda_1 = \int_\alpha \frac{dx}{y}$ and $\lambda_2 = \int_\beta \frac{dx}{y}$.)

Moreover, thinking of E in $\mathbb{P}^2$ "forces all lines to meet E in exactly three points". For example, the x-axis meets E in $(e_1, 0)$, $(e_2, 0)$, $(e_3, 0)$, and you can think of a vertical line as meeting E in o, (x_0, y_0), $(x_0, -y_0)$. To make this work in general you have to think of a tangent line as meeting E twice at a point of tangency (for an inflection point, three times); "three points" is meant in the sense of adding up these multiplicities:



The reason this works is that "restricting a cubic equation to a line gives a cubic polynomial", which has three solutions (over $\mathbb{C}$ or any other *algebraically closed* field).

[1] not an ellipse!! The reason for the terminology "elliptic" here is historical and somewhat obscure, having to do with the integral below being related to one that computes the arclength of an actual ellipse.

The group law. OK, so let's do some math. Let $K \subseteq \mathbb{C}$ be a subfield (e.g. $\mathbb{Q}$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{R}$, $\mathbb{C}$) and

$$p = (x_p, y_p)\,,\ q = (x_q, y_q)\ \in\ E(K);$$

that is, x_p, y_p, x_q, y_q belong to K and p, q both satisfy the equation (43):

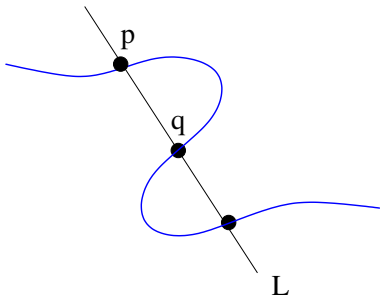
$$y_p^2 = x_p^3 + Ax_p + B\,, \quad y_q^2 = x_q^3 + Ax_q + B.$$

Take

$$L(K) = \{(x, y) \in K^2 \mid y = ax + b\}$$

to be the line through p and q; in particular,

$$y_p = ax_p + b \ \text{ and } \ y_q = ax_q + b.$$



Since $E(K) \cap L(K) \supset \{p, q\}$, we must have (for some $\tilde{x}$)

$$x^3 + Ax + B - (ax + b)^2 = (x - x_p)(x - x_q)(x - \tilde{x}), \tag{44}$$

which implies that

$$(\tilde{x}, \tilde{y}) := (\tilde{x}, a\tilde{x} + b) \text{ yields a third solution}$$

(regardless of whether K is algebraically closed) to the Weierstrass equation. Note that a is the slope of L.

Expanding (44) yields

$$x^3 - a^2x^2 + (A - 2ab)x + (B - b) = x^3 - (x_p + x_q + \tilde{x})x^2 + \cdots$$

$$\implies \ a^2 = x_p + x_q + \tilde{x}$$

$$\begin{aligned} \Longrightarrow \quad \tilde{x} &= a^2 - x_p x_q \\ &= \left(\tfrac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q \end{aligned}$$

$$\begin{aligned} \underset{b = y_p - a x_p}{\Longrightarrow} \quad \tilde{y} &= a(\tilde{x} - x_p) + y_p \\ &= \left(\tfrac{y_q - y_p}{x_q - x_p}\right)(\tilde{x} - x_p) + y_p. \end{aligned}$$

This gives the formula for the third intersection point as long as $x_p \neq x_q$. In the latter case, either $(x_q, y_q) = (x_p, -y_p)$ and the third intersection is o; or $p = q$ and L is the tangent line at x_p. To calculate the slope of the tangent line we write (by implicit differentiation of (43))

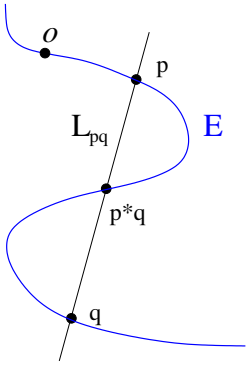
$$2ydy = (3x^2 + A)dx \quad \Longrightarrow \quad a = \left.\frac{dx}{dy}\right|_{(x_p, y_p)} = \tfrac{3x_p^2 + A}{2y_p}$$

$$\begin{aligned} \Longrightarrow \tilde{x} &= \left(\tfrac{3x_p^2 + A}{2y_p}\right)^2 - 2x_p, \\ \tilde{y} &= \left(\tfrac{3x_p^2 + A}{2y_p}\right)(\tilde{x} - x_p) + y_p, \end{aligned}$$

which yields the formula for the third intersection point when $p = q$.

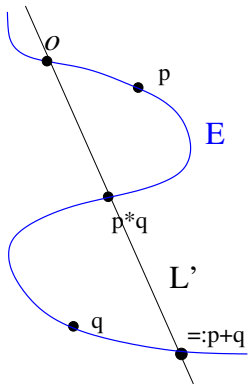
To define the group law, given $p, q \in E(K)$ we set

$$p * q := (\tilde{x}, \tilde{y}) = \text{third intersection point of } L_{pq} \text{ and } E :$$



Step 1

Then, we draw the line through o and $p * q$, and define $p + q$ to be the third intersection point of *that* line with E:

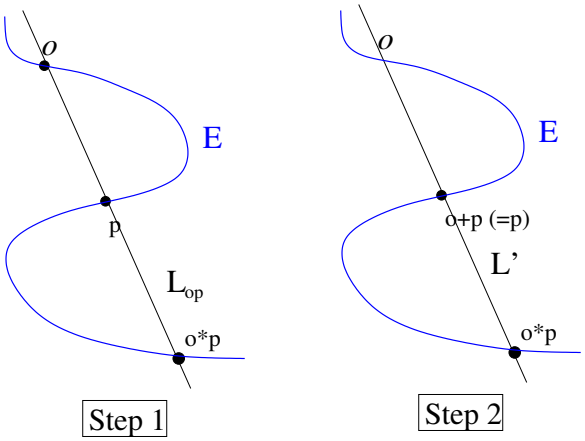


Of course, while this in fact makes sense for any cubic curve, for the Weierstrass ellipti curves we're studying L' is just the vertical line through $p * q = (\tilde{x}, \tilde{y})$, and so $p + q = (\tilde{x}, -\tilde{y})$.

By the formulas above, $x_p, y_p, x_q, y_q \in K \implies \tilde{x}, \tilde{y} \in K$ and so we conclude

THEOREM 199. *$E(K)$ is closed under "+", and so we have defined a binary operation on $E(K)$ (for any field $K \subset \mathbb{C}$).*

Actually there is one thing we haven't tried. What happensif we add o to $p = (x_p, y_p)$?

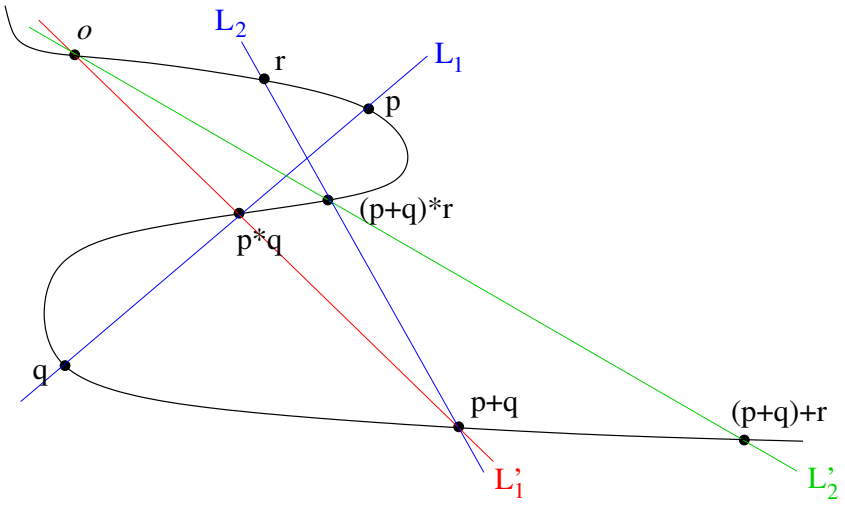


We get $o + p = p$, i.e. o is the "identity element". (In the special case where $p = o$, then both lines are the line at infinity, which hits

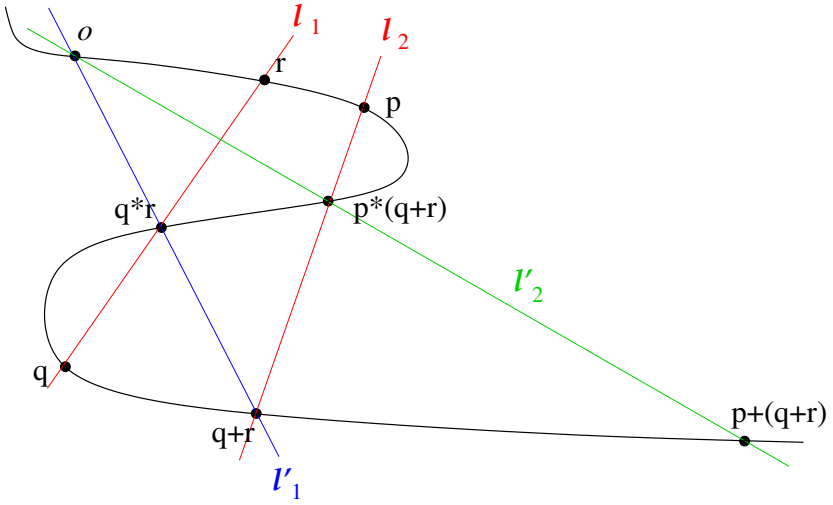
o "3 times" since o is an inflection point of E.) It is clear also that $p * q = q * p$ so $p + q = q + p$.

Next, given $p := (x_p, y_p)$, write $-p := (x_p, -y_p)$. The line $L = L_{p,-p}$ is vertical and the third intersection point is $p * (-p) = o$; hence $L' = L_{o,o} = L_\infty$ and $p + (-p) = o$. So inverses exist.

Finally, what about $(p + q) + r = (p + q) + r$, i.e. associativity? It clearly suffices to check that $(p + q) * r$



equals $p * (q + r)$:



A union of three lines is a cubic curve, so we have three cubics:

$$E,\ \ C := L_1 \cup \ell_1' \cup L_2,\ \text{ and } D := \ell_1 \cup L_1' \cup \ell_2,$$

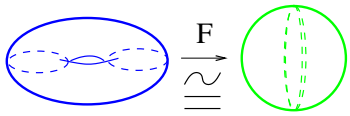
where the components of C are drawn in blue and those of D in red. The *Cayley-Bacharach Theorem* (which we won't prove carefully) says that if $D \cap E$ and $C \cap E$ have 8 points in common (each intersection has 9), then they are the same. Here, the 8 points are

$$p,\ q,\ r,\ p+q,\ q+r,\ p*q,\ q*r, \text{ and } o;$$

so $(p+q)*r$ and $p*(q+r)$ (the 9th points of the respective intersections) are forced to agree. This gives

THEOREM 200. *$(E(K), +, o)$ is an abelian group.*

The idea of why Cayley-Bacharach holds is that you can divide the equations of C and D (restricted to E) to get a meromorphic function on $E(\mathbb{C})$, $F := \frac{f_C}{f_D}$. The zeroes are where E meets C, the poles where E meets D. All of these cancel at the 8 common points. If the last 2 don't cancel, then F is not constant, and has one zero and one pole. With a little complex analysis one deduces from this that F maps $E(\mathbb{C})$ to $\mathbb{P}^1 := \mathbb{C} \cup \{\infty\}$ (topologically a sphere) in 1-to-1 fashion:



This is topologically impossible!

Exercises

(1) For this and the next 2 problems, consider the elliptic curve E with equation $y^2 = x^3 + x$. Write down the formulas explicitly for $p+q$ and $2p$ (x and y coordinates in terms of those of p and q).
(2) Show that $(1, \sqrt{2}) \in E(\mathbb{C})$ has order 4 under the group law; we call this a "4-torsion point". Consider the automorphism μ of

$E(\mathbb{C})$ given by $\mu(x, y) := (-x, iy)$ (called a "complex multiplication"). Use this to produce 3 more 4-torsion points. Can you use the group law to find them all? (If not, why?)

(3) Consider a point P of E with rational x-coordinate $x_0 = \frac{p}{2^a q}$, where the fraction is written in lowest terms, a is an odd natural number, and p and q are odd integers. Show that P has infinite order in the group law. [Hint: write (x_0, y_0) for this point, and let $(x_1, y_1) := 2(x_0, y_0)$ under the group law. Rewriting (if necessary) your formula from (6) as a formula for x_1 in terms of x_0 and simplifying, show that x_1 is of the same form, but with larger a. Then suppose the starting point was an N-torsion point for some N and produce a contradiction via the pigeonhole principle.]

(4) Write $X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3)$. Prove that $4A^3 + 27B^2 = 0 \iff \{e_i\}$ not all distinct.

CHAPTER 24

Elliptic curves over $\mathbb{F}_p$

Consider a cubic equation of the form

$$E:\ y^2 = x^3 + Ax + B\ (=: P(x)),\quad A, B \in \mathbb{Z}.$$

We can apply the last lecture's results to get a group structure on $E(\mathbb{Q})$, but "$E(\mathbb{Z})$" may not be closed under "+". That is, the set of points with integer coordinates isn't in general a subgroup of $E(\mathbb{Q})$, though it does contain the *torsion* subgroup (consisting of all elements of finite order).

Let p be an odd prime. If we define $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$,

$$E(\mathbb{F}_p) := \left\{ (x,y) \in \mathbb{F}_p \times \mathbb{F}_p \,\middle|\, y^2 \underset{(p)}{\equiv} x^3 + Ax + B \right\} \cup \{o\},$$

then there isn't necessarily a 2-tuple $(\tilde{x}, \tilde{y}) \in E(\mathbb{Z})$ (or even $E(\mathbb{Q})$) reducing (mod p) to $(x,y) \in E(\mathbb{F}_p)$, either. Consequently, if we want a group law on $E(\mathbb{F}_p)$, we need to check that the construction in the previous lecture still works.

First, we will want to be working with a *nonsingular* curve. In general, given a curve C_f defined by $f(x,y) \underset{(p)}{\equiv} 0$, the *multiplicity* of a point $(x_0, y_0) \in C_f(\mathbb{F}_p)$ is the largest integer μ such that $\left((\frac{\partial}{\partial x})^i (\frac{\partial}{\partial y})^j f \right)(x_0, y_0) \underset{(p)}{\equiv} 0$ for $i + j < \mu$. A *singularity* is a point of multiplicity > 1.

PROPOSITION 201. $\Delta := 4A^3 + 27B^2 \underset{(p)}{\not\equiv} 0 \implies$ *E is nonsingular over $\mathbb{F}_p$. (We say that E "has good reduction" mod p.)*

SKETCH. If E is singular, then there must exist (x_0, y_0) such that $y_0^2 - x_0^3 - Ax_0 - B \underset{(p)}{\equiv} 0$ and $2y_0 \underset{(p)}{\equiv} 0 \underset{(p)}{\equiv} 3x_0^2 + A$. Since 2 is invertible

mod p, we have $y_0 \underset{(p)}{\equiv} 0$ hence $x_0^3 + Ax_0 + B \underset{(p)}{\equiv} 0 \underset{(p)}{\equiv} 3x_0^2 + A \implies (x - x_0)^2 \mid x^3 + Ax + B$ in $\mathbb{F}_p[x] \implies x^3 + Ax + B \underset{(p)}{\equiv} (x - x_0)^2(x - x')$. For the x^2 term to be zero we must have $x' = -2x_0$ so

$$x^3 + Ax + B \underset{(p)}{\equiv} (x - x_0)^2(x + 2x_0) = x^3 - 3x_0^2 x - 2x_0^3$$

$$\implies A \underset{(p)}{\equiv} -3x_0^2 \text{ and } B \underset{(p)}{\equiv} -2x_0^3 \implies 4A^3 + 27B^2 \underset{(p)}{\equiv} -108x_0^6 + 108x_0^6 = 0.$$ □

REMARK 202. In the nonsingular case, it will turn out that there is a group homomorphism $E(\mathbb{Q}) \to E(\mathbb{F}_p)$, though (as indicated above) it is not in general surjective.

Before getting into the group law, we can try to count points:

PROPOSITION 203. *$|E(\mathbb{F}_p)| = p + 1 + a_p$, where a_p denotes the sum*

$$a_p := \sum_{\alpha \in \mathbb{F}_p} \sigma_p(\alpha) := \sum_{\alpha \in \mathbb{F}_p} \left(\frac{\alpha^3 + A\alpha + B}{p} \right)$$

of Legendre symbols.

PROOF. To count the points in $E(\mathbb{F}_p)$, we let α run through all elements of $\mathbb{F}_p$ and ask (for each α) for how many $\beta \in \mathbb{F}_p$ we have $(\alpha, \beta) \in E(\mathbb{F}_p)$ (i.e. $\beta^2 = \alpha^3 + A\alpha + \beta$). We add these up, then add 1 for the point "o" at infinity.

If $\sigma_p(\alpha) = 1$, then there exists $\beta \in \mathbb{F}_p^*$ such that $\beta^2 = \alpha^3 + A\alpha + \beta$; in this case, the points (α, β) and $(\alpha, -\beta)$ belong to $E(\mathbb{F}_p)$, and we get a contribution of 2.

If $\sigma_p(\alpha) = 0$, then $(\alpha, 0) \in E(\mathbb{F}_p)$, and the contribution is 1.

If $\sigma_p(\alpha) = -1$, then there does not exist a beta such that $(\alpha, \beta) \in E(\mathbb{F}_p)$, and the contribution is 0.

So the number of points is $1 + \sum_\alpha (\sigma_p(\alpha) + 1) = 1 + p + \sum_p \sigma_p(\alpha)$. □

A basic result (which we won't prove) is the **Hasse bound**:

THEOREM 204 (Hasse, 1933). *$|a_p| \leq 2\sqrt{p}$.*

Now we want to analyze intersections of lines and curves over $\mathbb{F}_p$. Recall (Corollary (II.F.2)) that a nonzero polynomial $P(x) \in \mathbb{F}_p[x]$ of degree n has at most n roots, counted with multiplicity. Define the **intersection multiplicity** of

$$L:\ g(x,y) := y - \{mx + r\} \underset{(p)}{\equiv} 0$$

with

$$C:\ f(x,y) \underset{(p)}{\equiv} 0$$

at $(x_0, y_0) \in L(\mathbb{F}_p) \cap C(\mathbb{F}_p)$ to be the largest integer M such that $f(x, mx + r) \underset{(p)}{\equiv} (x - x_0)^M k(x)$. We say that L is **tangent** to C at (x_0, y_0) if $M \geq 2$.

Let C (i.e. f) be of degree n.

PROPOSITION 205. *If the sum of intersection multiplicies of points in $L(\mathbb{F}_p) \cap C(\mathbb{F}_p)$ exceeds n, then $f = g \cdot h$ in $\mathbb{F}_p[x]$ and $C = L \cup \{$curve of degree $n - 1\}$.*

PROOF. The hypothesis means that $f(x, mx + r)$ has more than its degree in roots, counted with multiplicity, in contradiction to Cor. II.F.2 unless *it is identically zero*. Now, the division algorithm for *polynomials in y* over $\mathbb{F}_p[x]$ gives

$$f(x,y) = \underbrace{(y - mx - r)}_{g(x,y)} h(x,y) + r(x).$$

(Since we are dividing g into f, with g of degree 1 in y, the remainder r must have degree 0 in y, i.e. it is constant with respect to y.) Substituting $y = mx + r$ gives

$$0 \equiv f(x, mx + r) = 0 \cdot h(x, mx + r) + r(x) = r(x)$$

$\implies r(x)$ identically zero $\implies f = g \cdot h$. □

PROPOSITION 206. *If $(x_1, y_1), \ldots, (x_{n-1}, y_{n-1})$ are points in $L(\mathbb{F}_p) \cap C(\mathbb{F}_p)$, repeated according to their multiplicity, then there is an n^{th} point of intersection.*

PROOF. By hypothesis $P(x) = f(x, mx + r)$ has $n - 1$ solutions in $\mathbb{F}_p$. Repeated application of the division algorithm now gives

$$a_n x^n + a_{n-1}x^{n-1} + \cdots = P(x) = (x - x_1)(x - x_2)\cdots(x - x_{n-1})q(x),$$

where $q(x)$ is clearly of the form $a_n(x - x_n)$. Explicitly, we have

$$x_n = -a_{n-1}a_n^{-1} - x_1 - \cdots - x_{n-1} (\in \mathbb{F}_p),$$

and $(x_n, mx_n + r)$ gives an n^{th} solution. □

The upshot is that we may construct as in §IV.F the binary pairing on $E(\mathbb{F}_p)$, using $L_{PQ}(\mathbb{F}_p) \cap E(\mathbb{F}_p) = \{P, Q, P * Q\}$ (where $P * Q$ exists by Prop. 206) and so on. We again wind up with the formulas

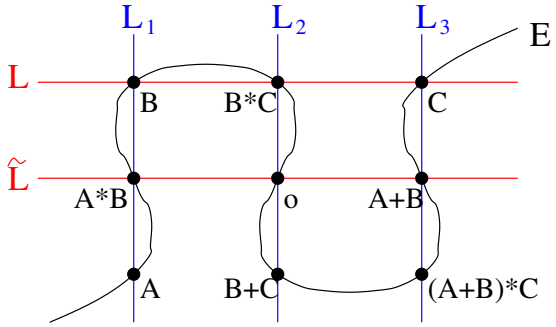
$$\text{(45)} \qquad \begin{cases} x_{P+Q} = & \left(\dfrac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q \\ y_{P+Q} = -\left(\dfrac{y_Q - y_P}{x_Q - x_P}\right)(x_{P+Q} - x_P) - y_P \end{cases}$$

and

$$\text{(46)} \qquad \begin{cases} x_{2P} = & \left(\dfrac{3x_P^2 + A}{2y_P}\right)^2 - 2x_P \\ y_{2P} = -\left(\dfrac{3x_P^2 + A}{2y_P}\right)(x_{2P} - x_P) - y_P. \end{cases}$$

Everything works as before except for associativity, where we shall require a more "algebraic"

PROOF (SKETCH). Use the diagram:



where (as before) E is defined by vanishing of $f(x,y) = y^2 - x^3 - Ax - B$. For simplicity we wll assume that the 9 points displayed are distinct, and that $p > 3$.

We want to show that $(A+B)+C = A+(B+C)$, or equivalently that $(A+B)*C = A*(B+C)$, which is just the statement that the bottom three displayed points are collinear. Put $C_g = L_1 \cup L_2 \cup L_3$, with equation $g := \ell_1\ell_2\ell_3 = 0$ (with $\ell_i(x,y)$ linear). Since f is irreducible, by Prop. 205 $C_g(\mathbb{F}_p) \cap E(\mathbb{F}_p)$ has nine intersection points (counted with multiplicity).

Let $P_0 \in L(\mathbb{F}_p)\backslash\{B, C, B*C\}$ and set $\alpha := -\frac{g(P_0)}{f(P_0)}$, $h := \alpha f + g$. Clearly $C_h(\mathbb{F}_p)$ contains the nine points above as well as P_0; indeed, it meets L in *four* points. By Prop. 205 we therefore have $h = \ell \cdot q$ for some quadratic polynomial q; the conic $C_q(\mathcal{F}_q)$ it defines must contain $o, A*B, A+B, A, B+C, (A+B)*C$ (since h vanishes on these and ℓ does not). But then $\tilde{L}$ meets C_q in the three points $o, A+B, A*B$, and so (again by Prop. 205) q factors as a product of linear polynomials $\tilde{\ell}\cdot\hat{\ell}$, where $\tilde{\ell}$ defines $\tilde{L}$. In particular, the line $\hat{L}$ defined by $\hat{\ell}$ must contain the remaining points $A, B*C, (A+B)*C$. Hence they are collinear. □

So we arrive at:

THEOREM 207. *The pairing given by* (45)-(46) (*i.e.* "+") *defines the structure of a finite abelian group on* $E(\mathbb{F}_p)$.

EXAMPLE 208. Let E denote the curve defined by

$$y^2 = x^3 - 2x - 3$$

over $\mathbb{F}_7$. We have $P := (3,2) \in E(\mathbb{F}_7)$, as it solves the congruence equation ($2^2 \underset{(7)}{\equiv} 3^3 - 2\cdot 3 - 3$). One computes $2P = (2,6)$, $3P = 2P + P = (4,2)$, $4P = (0,5)$, $5P = (5,0)$, $6P = (0,2)$, $7P = (4,5)$, $8P = (2,1)$, $9P = (3,5)$, $10P = (3,2) + (3,5) = o$ (since they have the same x-coordinate). That is, P has order 10 and we have found a cyclic subgroup[1] $\mathbb{Z}_{10} \leq E(\mathbb{F}_7)$.

[1]where I am writing $\mathbb{Z}_m$ for the group $(\mathbb{Z}/m\mathbb{Z}, +, 0)$.

There are two ways to see that these are all of the points: forst, we could check that the Legendre symbol $\left(\frac{x^3-2x-3}{7}\right) = 1$ only for $x = 0, 2, 3, 4, 5$, and is otherwise -1.

Alternatively, the Hasse bound $||E(\mathbb{F}_7)| - (p+1)| < 2\sqrt{p}$ implies

$$||E(\mathbb{F}_7)| - 8| \leq 5. \tag{47}$$

If $|E(\mathbb{F}_7)| > 10$, then $|E(\mathbb{F}_7)|/|\mathbb{Z}_{10}|$ has to be an integer > 1 (by Lagrange's theorem); hence $|E(\mathbb{F}_7)| \geq 20$, impossible by (47).

We conclude that $E(\mathbb{F}_7) \cong \mathbb{Z}_{10}$.

EXAMPLE 209. Here is a much richer example of computing group structure of $E(\mathbb{F}_p)$. We will look at the curve E with equation

$$y^2 = x^3 - x$$

over the field $\mathbb{F}_{71}$. To compute the order, note that $(-1)^{\frac{71-1}{2}} = (-1)^{35} = -1 \underset{(71)}{\not\equiv} 1 \implies -1$ is not a square mod $71 \implies$

$$\left(\frac{-\alpha}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{\alpha}{71}\right) = -\left(\frac{\alpha}{71}\right).$$

So for any odd function $f(x)$ (such as $x^3 - x$), $\sum_{\alpha\in\mathbb{F}_{71}}\left(\frac{f(\alpha)}{71}\right)$ splits into $\sum_{\alpha=1}^{35}\left(\frac{f(\alpha)}{71}\right)$ and $\sum_{\alpha=36}^{70}\left(\frac{f(\alpha)}{71}\right) = \sum_{\alpha=1}^{35}\left(\frac{f(-\alpha)}{71}\right) = \sum_{\alpha=1}^{35}\left(\frac{-f(\alpha)}{71}\right) = -\sum_{\alpha=1}^{35}\left(\frac{f(\alpha)}{71}\right)$, which then cancel term by term. By Proposition 203, we therefore have

$$|E(\mathbb{F}_{71})| = 71 + 1 + \sum_{x\in\mathbb{F}_{71}}\left(\frac{x^3-x}{71}\right) = 72 = 8 \times 9.$$

Now given any $P \in E(\mathbb{F}_{71})$, setting $Q := -8P$, $R := 9P$ gives $P = Q + R$, with $8R = o$ and $9Q = o$. Moreover, if $T \in E(\mathbb{F}_{71})$ has $8T = o$ and $9T = o$, then $T = 9T - 8T = o - o = o$. So we have an isomorphism of groups

$$E(\mathbb{F}_{71}) \cong E_2 \times E_3,$$

where $E_2 := \{P \in E(\mathbb{F}_{71}) \mid 8P = o\}$ and $E_3 := \{P \in E(\mathbb{F}_{71}) \mid 9P = o\}$ are the *primary components* of $E(\mathbb{F}_{71})$. Since orders of elements must divide the order of a group, we see that there is no option but to have $|E_2| = 8$, $|E_3| = 9$. As they are abelian, the only possibilities are[2]

(i) $E_2 \cong \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

and

(ii) $E_3 \cong \mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

For (i), let's figure out the 2-torsion points, i.e. $P\,(\neq o)$ such that $2P = o$. This means $P = -P$, i.e. $(x_P, -y_P) = (x_P, y_P)$, which implies $y_P = 0$. But the roots of $x^3 - x$ over $\mathbb{F}_{71}$ are exactly $x = 0, 1, -1$, and so there are three 2-torsion elements of $E(\mathbb{F}_{71})$. These belong to E_2. Now, $\mathbb{Z}_8$ has one 2-torsion element (namely, 4), $\mathbb{Z}_2 \times \mathbb{Z}_4$ has three (namely, $(1,0)$, $(0,2)$, and $(1,2)$), while $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has seven (every element but $(0,0,0)$). So

$$E_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_4.$$

For (ii), try to find the 3-torsion points, i.e. those with $3P = o$ (and $P \neq o$) This is the same as $-2P = P \implies x_{2P} \underset{(71)}{\equiv} x_P \implies \left(\frac{3x_P^2-1}{2y_P}\right)^2 - 2x_P \underset{(71)}{\equiv} x_P \implies 3x^4 - 6x^2 + 1 \underset{(71)}{\equiv} 0$. This has at most four roots, which come in pairs $\{r, -r\}$. Since $(-r)^3 - (-r) = -(r^3 - r)$, and the Legendre symbol $\left(\frac{-1}{71}\right) = -1$, both can't lead to a point on $E(\mathbb{F}_{71})$. Hence there are at most two x-values which can be the x-coordinate of a 3-torsion point, hence at most four 3-torsion points (think $\pm y$). Now, $\mathbb{Z}_9$ has two and $\mathbb{Z}_3 \times \mathbb{Z}_3$ has eight (impossible). So

$$E_3 \cong \mathbb{Z}_9,$$

and we conclude that

$$E(\mathbb{F}_{71}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \cong \mathbb{Z}_2 \times \mathbb{Z}_{36}.$$

[2]Here I use the shorthand $\mathbb{Z}_n$ for the finite cyclic group $(\mathbb{Z}/n\mathbb{Z}, +, 0)$.

Exercises

(1) Let E be defined by $y^2 = x^3 + x + 1$. Compute the number of points in the group $E(\mathbb{F}_p)$ for $p = 3$, 5, 7, and 11. In each case verify Hasse's bound $|a_p| < 2\sqrt{p}$, where $a_p = |E(\mathbb{F}_p)| - p - 1$.

(2) With E as in (1), $P = (4, 2)$ and $Q = (0, 1)$ belong to $E(\mathbb{F}_5)$. Find n such that $nP = Q$.

(3) Let E be an eliptic curve over $\mathbb{F}_p$, and $P, Q \in E(\mathbb{F}_p)$. Assume $Q \in \langle P \rangle$ and let $n_0 > 0$ be the smallest solution to $nP = Q$, and $s > 0$ be the smallest solution to $sP = o$. Prove that every solution to $Q = nP$ takes the form $n_0 + is$ for some $i \in \mathbb{Z}$. [Hint: Write n as $is + r$ for some $0 \leq r < s$ and determine the value of r.]

(4) Let E be the elliptic curve $y^2 = x^3 - x$. Find the group structure of $E(\mathbb{F}_5)$ and $E(\mathbb{F}_{11})$.

Part 5

Elliptic cryptosystems

CHAPTER 25

Elliptic curve discrete log problem (ECDLP)

The idea behind elliptic curve cryptography is to exploit the analogy between the two finite abelian groups

$$((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1) \text{ and } \left(E(\mathbb{F}_p), +, o\right),$$

so as to replace cryptosystems based on the former with ones based on the latter.

Let G be a group, $g, h \in G$ with $h \in \langle g \rangle$. (We will write the binary operation as multiplication, though in the application to elliptic curves it will be addition.) Then there exists $n \in \mathbb{Z}$ with

$$g^n = h. \tag{48}$$

If the order of $\langle g \rangle$ is finite (=: N), then it isn't unique – any $n + Nk$ will work – but becomes so if we view the solution in $\mathbb{Z}/N\mathbb{Z}$.

Given an elliptic curve

$$E: \ y^2 = x^3 + Ax + B \quad (A, B \in \mathbb{Z})$$

where $p \nmid \Delta (= 4A^3 + 27B^2)$, $(E(\mathbb{F}_p), +, o)$ is a finite abelian group. Given also two points $P, Q \in E(\mathbb{F}_p)$, we can ask for the solution to

$$nP = Q. \tag{49}$$

Now, this may not make sense:

- $E(\mathbb{F}_p)$ may not be cyclic;
- even if it is, P need not generate it.

So one has to assume $Q \in \langle P \rangle$. With this assumption, and writing $N = |\langle P \rangle|$, there exists a unique solution

$$n =: \log_P(Q) \in \mathbb{Z}/N\mathbb{Z}$$

to (49). This is, of course, a special case of (48).

REMARK 210. One may think of this "elliptic discrete log" as defining an isomorphism

$$\log_P : \langle P \rangle \to \mathbb{Z}/N\mathbb{Z}$$

of groups (where $\langle P \rangle$ is a subgroup of $E(\mathbb{F}_p)$). Why? If $\log_P Q_1 = n_1$, and $\log_P Q_2 = n_2$, then $Q_1 = n_1 P$ and $Q_2 = n_2 P$

$$\implies \quad Q_1 + Q_2 = n_1 P + n_2 P$$

$$= (\underbrace{P + \cdots + P}_{n_1}) + (\underbrace{P + \cdots + P}_{n_2}) = \underbrace{P + \cdots + P}_{n_1+n_2} = (n_1 + n_2)P$$

$$\implies \quad \log_P(Q_1 + Q_2) = n_1 + n_2 = \log_P Q_1 + \log_P Q_2$$

and so $\log_P$ is a group homomorphism. That it's a bijection is clear.

REMARK 211. To compute nP quickly, we may use "double-and-add", writing n in binary $n_0 + n_1 \cdot 2 + \cdots + n_r \cdot 2^r$ (all n_i 0 or 1) and computing

$$nP = n_0 P + n_1(2P) + n_2 2(2P) + \cdots + n_r 2(2^{r-1}P),$$

or using the analogue of the low-storage fast-powering algorithm. But it is faster to allow $n_i = -1, 0$, or 1: e.g.

$$15 = 2^4 - 1 = 1 + 2 + 2^2 + 2^3,$$

since $-P = -(x, y) = (x, -y)$ in $E(\mathbb{F}_p)$ is trivial to compute.[1]

PROPOSITION 212. *For $n \in \mathbb{N}$, $k = \lfloor \log_2 n \rfloor + 1$, we may write $n = u_0 + 2u_1 + 2^2 u_2 + \cdots + 2^k u_k$ with $u_i \in \{-1, 0, 1\}$ and at most $\frac{1}{2}k$ of the u_i nonzero.*

PROOF. Write n in binary then use (working left to right)

$$2^s + 2^{s+1} + \cdots + 2^{s+k-1} = 2^s(2^t - 1) = -2^s + 2^{s+t}$$

to introduce gaps. □

[1] compare to computing inverses in $(\mathbb{Z}/m\mathbb{Z})^*$

Babystep-giantstep for ECDLP. There is no subexponential-time algorithm to solve the ECDLP (49), outside of special cases (like $|E(\mathbb{F}_p)| = p$): basically, your options are the collision-type algorithms for DLP, like Shanks or a reworking of Pollard ρ (which we set up for factoring way back in §II.D) for DLP.

EXAMPLE 213. Let $p = 73$. Consider the curve

$$E: \ Y^2 = X^3 + \underbrace{8}_{A} X + \underbrace{7}_{B}$$

over $\mathbb{F}_p$; the points $P = (32, 53)$ and $Q = (39, 17)$ belong to $E(\mathbb{F}_p)$. We want to determine $\log_P Q$.

Let's try an elliptic version of Shanks's babystep-giantstep algorithm. First, by Hasse's theorem, the order of $E(\mathbb{F}_p)$ hence of $\langle P \rangle$ is no more than $N = p + 1 + \lfloor 2\sqrt{p} \rfloor = 73 + 1 + 17 = 91$. Hence we can take $m = 1 + \lfloor \sqrt{N} \rfloor = 1 + 9 = 10$ in Shanks, and the two lists are:

- o, P, $2P$, ..., $10P$ (which turns out to be $(29, 10)$); and
- Q, $Q - 10P$, $Q = 2(10P)$, ..., $Q - 10^2 P$.

Now

$$Q - 10P = (39, 17) - (29, 10) = (\underbrace{39}_{x_1}, \underbrace{17}_{y_1}) + (\underbrace{29}_{x_2}, \underbrace{-10}_{y_2}) =: (x_3, y_3)$$

may be computed by the formulas (IV.G.1) using the slope $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{27}{10} \underset{(73)}{\equiv} 10$ (since $10^2 = 100 \underset{(73)}{\equiv} 27$). This gives

$$x_3 = \lambda^2 - x_1 - x_2 = 100 - 39 - 29 = 32 \ \text{ and}$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 10(39 - 32) - 17 = 70 - 17 = 53,$$

and so the match between the lists happens at the very beginning:

$$Q - 10P = (32, 53) = P.$$

Hence $Q = 11P$, i.e. $\log_P Q = 11$, is the solution to the ECDLP.

Pollard rho for DLP. I'd now like to explain how Pollard's ρ method gets adapted to an abstract discrete logarithm problem, and why running time is (like Shanks) essentially $\mathcal{O}(\sqrt{N})$ hence $\mathcal{O}(\sqrt{p})$.

Let $\mathscr{S}$ be a set, and $f : \mathscr{S} \to \mathscr{S}$ a "sufficiently random" function. Let $x_0 \in \mathscr{S}$, and define two sequences recursively by

$$x_i := f(x_{i-1})$$

and

$$y_0 := x_0\,, \;\; y_i := f(f(y_{i-1}))\,(= x_{2i}).$$

Suppose

$$x_j = x_i \iff i \geq T \text{ and } j \underset{(M)}{\equiv} i \;:$$

Then

$$x_{2i}(= y_i) = x_i \iff i \geq T \text{ and } M \mid i,$$

which happens for some $i < T + M$.

How large do we likely have to take i to get such a match, given $N = |\mathscr{S}|$? Well, with the assumption on f, the probability[2]

$$\begin{aligned}
\pi\left(x_0, \ldots, x_{k-1} \text{ distinct}\right) &= \prod_{i=1}^{k-1} \pi\left(\begin{array}{c|c} x_j \neq x_i & x_0, \ldots, x_{i-1} \\ \forall 0 \leq j < i & \text{distinct} \end{array} \right) \\
&= \prod_{i=1}^{k-1} \frac{N-i}{N} \\
&= \prod_{i=1}^{k-1} \left(1 - \frac{i}{N}\right) \\
&< \prod_{i=1}^{k-1} e^{-\frac{i}{N}} \;\; = \;\; e^{-\frac{1+2+\cdots+(k-1)}{N}} \;\; = \;\; e^{\frac{k^2-k}{2}} \\
&< e^{-\frac{k^2}{2N}}
\end{aligned}$$

$$\implies \pi\left(\text{a match in the first } k \text{ steps}\right) > 1 - e^{-\frac{k^2}{2N}}$$

$$\implies \pi\left(\text{a match in the first } 3\sqrt{N} \text{ steps}\right) > 1 - e^{-\frac{9}{2}} > 0.98.$$

[2]Here $\pi(A)$ denotes the probability of an event A taking place, while $\pi(A \mid B)$ is the (conditional) probablity that A takes place if B does.

The specific function which is used to apply this to the discrete log problem (48) in $\mathbb{F}_p^*$ is

$$f(x) = \begin{cases} gx, & 0 \leq x < \frac{p}{3} \\ x^2, & \frac{p}{3} \leq x < \frac{2p}{3} \\ hx, & \frac{2p}{3} \leq x < p \end{cases}$$

(modulo p, of course) so that

$$\begin{cases} x_i = g^{\alpha_i} h^{\beta_i} \\ y_i = g^{\gamma_i} h^{\delta_i}. \end{cases}$$

When these match, we have

$$g^{\alpha_i - \gamma_i} \underset{(p)}{\equiv} h^{\delta_i - \beta_i} \left(= g^{n(\delta_i - \beta_i)} \right)$$

which assuming g a generator implies

$$(\alpha_i - \gamma_i) \underset{(p-1)}{\equiv} n(\delta_i - \beta_i).$$

Taking $d := (\delta_i - \beta_i, p-1)$, the Euclidean algorithm provides an s satisfying $s(\delta_i - \beta_i) \underset{(p-1)}{\equiv} d$, and thus

$$(\alpha_i - \gamma_i)s \underset{(p-1)}{\equiv} n(\delta_i - \beta_i)s \underset{(p-1)}{\equiv} nd. \tag{50}$$

Since d divides $(p-1)$, it must therefore divide the left-hand side of (50). Setting

$$\omega := \frac{(\alpha_i - \gamma_i)s}{d},$$

we divide (50) by d to obtain

$$\omega \underset{(\frac{p-1}{d})}{\equiv} n,$$

and conclude that n is one of

$$\omega,\ \omega + \tfrac{p-1}{d},\ \omega + 2\tfrac{p-1}{d},\ \ldots,\ \omega + (d-1)\tfrac{p-1}{d}$$

modulo $p-1$. Plug these in to $g^n = h$ to find the right one.[3]

In the exercises, you will be asked to adapt this to the ECDLP.

[3] see §4.5 in [HPS]

Index calculus. The fact the only $\sqrt{p}$ time algorithms are available for ECDLP is in marked contrast to the situation for the DLP in $\mathbb{F}_p^*$, which has a subexponential-time algorithm: the index calculus. (This makes elliptic curves apparently more secure for cryptography.) I will only give a rough idea of this here:[4] to solve $g^x \underset{(p)}{\equiv} h$, the first step is *solving* $g^x \underset{(p)}{\equiv} \ell$ *for all primes* $\ell \leq B$ (B not too large). To do this, compute $g_i :\underset{(p)}{\equiv} g^i$ for a random selection of exponents, keeping only the *B-smooth* results – i.e. those which may be written

$$g_i = \prod_{\ell \leq B} \ell^{u_\ell(i)},$$

so that applying $\log_g$ yields

$$i \underset{(p-1)}{\equiv} \sum_{\ell \leq B} u_\ell(i) \log_g(\ell).$$

Continue until there are $\pi(B)$ equations, and solve this linear system for the $\{\log_g(\ell)\}$.

The second step is to compute $hg^{-1}, hg^{-2}, hg^{-3}, \ldots$ until we reach a B-smooth number

$$hg^{-k} \underset{(p)}{\equiv} \prod_{\ell \leq B} \ell^{e_\ell}.$$

Taking $\log_g$ yields

$$\log_g h \underset{(p-1)}{\equiv} k + \sum_{\ell \leq B} e_\ell \log_g(\ell)$$

(where we know the $\{\log_g(\ell)\}$ from the previous step), solving the DLP.

What makes this work (quickly) is the *density* of B-smooth numbers, which involves the prime number theorem, and which has no analogue for general groups such as $E(\mathbb{F}_p)$.

[4] a discussion may be found in [HPS] §3.8

Exercises

(1) Adapt the Pollard ρ algorithm for the DLP (explained in §V.A) to the ECDLP. (Write out the algorithm and briefly justify why it works.)

CHAPTER 26

Elliptic curve cryptography

The difficulty of the ECDLP suggests that elliptic curves over finite fields should provide extra-secure encryption. Indeed, it turns out that with (roughly) a quarter of the digits, we can get the same level of security with $E(\mathbb{F}_p)$ as with $\mathbb{F}_p^*$ (say); but a quarter of the digits means vastly improved efficiency.

As a result, elliptic curves are used by governments, in your cell phones and on your computer. One technique that has been used by Microsoft to prevent music file-sharing, is to hide a private key in several files on your computer when you download a license to play a .wma file. Since the private key is required to decrypt the file, copying the .wma and license file onto another computer won't work. The encryption scheme is an *elliptic version of El Gamal*, using roughly 50 digit numbers for p, A, and B.

In some of the exercises, the values of p, A, and B get a little big for hand computation. I would recommend familiarizing yourself with commands *ellinit* and *ellpow* in PARI.

Elliptic Diffie-Hellman key exchange.
Step 1. Diffie and Hellman agree *publicly* on:

- $p =$ large prime;
- $E =$ elliptic curve over $\mathbb{F}_p$ (i.e. $A, B \in \mathbb{F}_p$ such that $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$); and
- $P \in E(\mathbb{F}_p)$.

Step 2.

- Diffie [resp. Hellman] choose (in secret) *private* integers n_D [resp. n_H];

- they compute and publicize $Q_D(=(x_D, y_D)) := n_D P$ [resp. $Q_H(=(x_H, y_H)) := n_H P$] in $E(\mathbb{F}_p)$.

Step 3.

- Diffie sees Q_H, computes $n_D Q_H = n_D n_H P$;
- Hellman sees Q_D, computes $n_H Q_D = n_H n_D P$.

In this way they arrive at a shared secret key.[1]

REMARK 214. They only need to send each other the x-coordinates x_D, x_H of Q_D, Q_H. This determines the point Q up to $\pm$ (in the group law on $E(\mathbb{F}_p)$). So for example, Diffie sends x_D, Hellman finds a y-value $\tilde{y}_D$ such that $\tilde{Q}_D := (x_D, \tilde{y}_D) \in E(\mathbb{F}_p)$; we then have $\tilde{y}_D = \pm y_D$ and $\tilde{Q}_D = \pm Q_D$. So when Hellman computes $n_H \tilde{Q}_D = n_H(\pm Q_D) = \pm(n_H Q_D)$ and Diffie similarly, they get the same point up to $\pm$ in the group law; in particular, *they get the same x-coordinate* and *this* is then what is used as the secret shared key.

REMARK 215. How do we quickly find y_0 completing $x_0 \in \mathbb{F}_p$ to $(x_0, y_0) \in E(\mathbb{F}_p)$, assuming one exists? That is, how do we efficiently find a square root of $\alpha := x_0^3 + Ax_0 + B$? Suppose $p \underset{(4)}{\equiv} 3$; if $\alpha = \beta^2$, then $\alpha^{\frac{p+1}{4}}$ satisfies $(\alpha^{\frac{p+1}{4}})^2 = \alpha^{\frac{p+1}{2}} = \beta^{p+1} = (\beta^{p-1})\beta^2 = \beta^2 = \alpha$ $\implies \alpha^{\frac{p+1}{4}} = \pm\beta$.

Elliptic El Gamal cryptosystem. There is no RSA for elliptic curves, since that would require being able to choose the order of the group to be pq. But the other main cryptosystem we devised generalizes nicely.

Here is the basic algorithm:

- Sender and Receiver agree publicly on p, E, and $P \in E(\mathbb{F}_p)$ as above.
- Receiver chooses a *private key* $n \in \mathbb{Z}$, computes and sends the *public key* $Q := nP$ to Sender.

[1] See [HPS] for numerical examples.

- Sender wants to send a plaintext *message* $M \in E(\mathbb{F}_p)$. To do this, s/he chooses a (private) *ephemeral key* $k \in \mathbb{Z}$, and computes/sends the *ciphertext* $(C_1, C_2) := (kP, M + kQ)$ to Receiver.
- Receiver decrypts the ciphertext, by computing $C_2 - nC_1 = M + kQ - nkP = M + knP - nkP = M$.

REMARK 216. What is a "message in $E(\mathbb{F}_p)$"? Even if one only "uses the x-coordinate" as message, you would have to be lucky to have your message (say x_0) satisfy that the Legendre symbol $\left(\frac{x_0^3+Ax_0+B}{p}\right) =$ 1 or 0 (not -1) – otherwise there is no point in $E(\mathbb{F}_p)$ with this x-coordinate!

REMARK 217. Sender cannot just send x-coordinates of C_1, C_2. Here the $\pm$ matters: for example, if Receiver reconstructed $-C_2$ instead of C_2 from its x-coordinate, s/he would get $-C_2 - nC_1 = -M - knP - nkP$ whose last 2 terms don't cancel out! This can be fixed by sending, instead of y-coordinate, a single bit (0 or 1) that tells which y-value to use:

$$\beta := \begin{cases} 0 & \text{if} \quad 0 \le y < \frac{1}{2}p \\ 1 & \text{if} \quad \frac{1}{2}p < y < p. \end{cases}$$

(Unless $y = 0$, y is in one interval iff $-y$ is in the other.) This is important because not having to send the y-coordinate cuts the message expansion ratio down from 4 to 2.

EXAMPLE 218. Let $p = 1123$, $E : y^2 = x^3 + 54x + 87$, and suppose we are sent the "point of $E(\mathbb{F}_p)$" $x_0 = 278$, $\beta_0 = 0$. What is y_0? We write $x_0^3 + 54x_0 + 87 = 278^3 + 54 \cdot 278 + 87 \underset{(1123)}{\equiv} 216$. Since $p \underset{(4)}{\equiv} 3$, we can find a square root of 216 by $216^{\frac{p+1}{4}} = 216^{281} \underset{(1123)}{\equiv} 487\ (< \frac{p}{2})$, while the other root is $-487 \underset{(1123)}{\equiv} 636\ (> \frac{p}{2})$. So $y_0 = 487$.

Coming back to Remark 216, there is an improvement of elliptic El Gamal due to Menezes and Vanstone, which allows for free choice

of message between 0 and $p-1$. The first two steps are the same. The third is:

- Sender wants to send plaintext values $m_1, m_2 \in \mathbb{F}_p$ S/he chooses an ephemeral key k, computes $R = kP \in E(\mathbb{F}_p)$ and $S = kQ = (x_S, y_S) \in E(\mathbb{F}_p)$, sets $c_i := x_S m_i \in \mathbb{F}_p$ $(i = 1, 2)$, and sends the ciphertext $(R, (c_1, c_2))$.
- Receiver computes $T = nR = (x_T, y_T)$, then recovers the message via $(x_T^{-1} c_1, y_T^{-1} c_2)$ (to be verified in an exercise).

Exercises

(1) Alice and Bob agree to use the elliptic Diffie-Hellman key exchange with the prime $p = 2671$, elliptic curve E: $Y^2 = X^3 + 171X + 853$, and point $P = (1980, 431) \in E(\mathbb{F}_p)$.
(a) Alice sends to Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. What point should Bob send to Alice?
(b) What is their secret shared value?
(c) How difficult is it for Eve to figure out Alice's secret multiplier n_A? (Try to find it using PARI.)
(d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the x-coordinate $x_A = 2$ of her point Q_A. Bob decides to use the secret multiplier $n_B = 875$. What single number modulo p should Bob send to Alice, and what is their secret shared value?

(2) [HPS] p. 342 #5.16

CHAPTER 27

Lenstra's factorization algorithm

While there isn't ann elliptic curve version of RSA, there is a very effective elliptic approach to factoring a large integer $N = pq$.

Let's first review how the Pollard $p-1$ method works, in the event that $p-1$ is B_0-smooth (and $q-1$ is not):

$$p - 1 = \prod_{\substack{\ell \leq B_0 \\ \ell \text{ prime}}} \ell^{m_\ell},$$

with $M := \max_{\ell \leq B_0}\{m_\ell \cdot \ell\}$. Then we have

$$(p-1) \mid M! \underset{\text{Fermat}}{\implies} a^{M!} \underset{(p)}{\equiv} 1 \implies p \mid (a^{M!} - 1).$$

Assuming $q \nmid (a^{M!} - 1)$, we conclude that $(a^{M!} - 1, N) = p$. Group-theoretically, what is going on here is (by the Chinese Remainder Theorem)

$$\begin{array}{rcccc} (\mathbb{Z}/N\mathbb{Z})^* & \cong & \overbrace{(\mathbb{Z}/p\mathbb{Z})^*}^{\text{order } p-1} & \times & \overbrace{(\mathbb{Z}/q\mathbb{Z})^*}^{\text{order } q-1} \\ a \pmod N & \mapsto & (a \pmod p & , & a \pmod q) \\ a^{M!} \pmod N & \mapsto & (1 \pmod p & , & \underbrace{a^{M!}}_{\underset{(p)}{\not\equiv 1}} \pmod q). \end{array}$$

On the other hand, if neither $p-1$ nor $q-1$ is B_0-smooth (for B_0 not too big), then Pollard is unlikely to work.

EXAMPLE 219. Let $B_0 = 20$, $N = 6313 = 59 \cdot 107 = p \cdot q$. Notice that $p - 1 = 58 = 2 \cdot 29$ and $q - 1 = 106 = 2 \cdot 53$ each have prime factors > 20. So it is no surprise that $(2^{20!} - 1, 6313) = 1$.

But suppose we could somehow replace $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ with a group of order $p - 2 = 57 = 3 \cdot 19$ – then we'd be in luck! This is the idea behind Lenstra's method: the order of the group $E(\mathbb{F}_p)$ is $p + 1 \pm s$ for $s \in \mathbb{Z}_{\geq 0}$ with $0 \leq s < 2\sqrt{p}$. Indeed, if E is $y^2 = x^3 + x + 54$, then (using Prop. IV.G.3) one can show that $|E(\mathbb{F}_{59})| = 57$, which looks promising for our example.

One very puzzling issue, however, is: what are we supposed to do *mod* N? After all, $\mathbb{Z}/N\mathbb{Z}$ isn't a field, so we can't expect

$$E(\mathbb{Z}/N\mathbb{Z}) := \{(x, y) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \mid y^2 \underset{(N)}{\equiv} x^3 + Ax + B\}$$

to be closed under the addition law! While the

$$x_{P+Q} := \lambda^2 - x_P - x_Q\,, \quad y_{P+Q} := \lambda(x_P - x_{P+Q}) - y_P$$

part isn't problematic, the

$$\lambda = \underbrace{\frac{y_Q - y_P}{x_Q - x_P}}_{\text{(distinct pts.)}} \text{ or } \underbrace{\frac{3x_P^2 + A}{2y_P}}_{\text{(pt. doubling)}} \tag{51}$$

certainly is, if $x_Q - x_P$ resp. $2y_P$ isn't in $(\mathbb{Z}/N\mathbb{Z})^*$ (i.e. not prime to N). All we can say is that

$$\begin{array}{ccc} E(\mathbb{Z}/N\mathbb{Z}) & \subset & \overbrace{E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})}^{\text{actual group}} \\ \underbrace{(x,y)}_{\text{mod } N} & \mapsto & (\underbrace{(x,y)}_{\text{mod } p}\,,\ \underbrace{(x,y)}_{\text{mod } q}) \end{array}$$

is some subset, at least at first glance.

But actually, we can describe exactly when point-adding on $E(\mathbb{Z}/N\mathbb{Z})$ fails. If (say) $p \mid (x_Q - x_P)$ in (51), then what happens if we add the reduction of those points (mod p) in $E(\mathbb{F}_p)$? We get o, by definition! So failure occurs *precisely when the sum of points gives* (o, R) *or* (R', o) *in* $E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z})$ (with R resp. $R' \neq o$).

Now suppose we were taking repeated "powers" of some $P \in E(\mathbb{Z}/N\mathbb{Z})$: $2P$, $3(2P) = (3!)P$, ..., up to $(B_0!)P$. If $|E(\mathbb{Z}/p\mathbb{Z})|$ (and hence the order of P mod p) divides $M!$ for some $M \leq B_0$, but the order of P in $E(\mathbb{Z}/q\mathbb{Z})$ does not divide $M!$, then in $E(\mathbb{F}_p) \times E(\mathbb{F}_q)$

we get $(M!P \pmod p, M!P \pmod q) = (o, R)$ (with $R \neq o$). Hence, at some point in the computation of $M!P$ in $E(\mathbb{Z}/N\mathbb{Z})$, we must run into a roadblock of the form $(x_{P'} - x_{Q'}, N) \neq 1$ when trying to use the Euclidean algorithm to invert $x_{P'} - x_{Q'} \pmod N$.

EXAMPLE 220. Again let $N = 6313$, and E be defined by $y^2 = x^3 + x + 54$, so that $E(\mathbb{Z}/59\mathbb{Z}) = 57 = 19 \cdot 3 \mid 19!$. In trying to compute $(19!)P$ for $P = (2, 8)$ (which turns out to be a generator of $E(\mathbb{F}_{59})$) we should "discover" the factor 59 of N. We will do this in PARI:

```
gp>       E=ellinit([0,0,0,1,54]*Mod(1,6313))
gp>       ellpow(E,[2,8]*Mod(1,6313),18!)
=[Mod(677,6313),Mod(262,6313)]            (no problem yet!)
gp>       ellpow(E,[677,262]*Mod(1,6313),19)
***ellpow:  impossible inverse modulo:  Mod(1298,6313)
gp>       gcd(1298,6313)
=59.
```

In general, it is not so easy to guess points on curves after you've written one down.There are two ways around this:

(1) Choose A and the point $P = (a, b)$ randomly, set $B := b^2 - a^3 - A - a$ so that $b^2 = a^3 + Aa + B$. (In some sense, this "lets the point determine the curve E".)
(2) Take elliptic curves only of the form $y^2 = x^3 + Ax + 1$, since these always have the point $P = (0, 1)$.

The following version of Lenstra's algorithm is very analogous to Pollard $(p - 1)$ and uses (1). (We take N to be given.)

Step 1 : Choose $A, a, b \in \mathbb{Z}/N\mathbb{Z}$ randomly.
Step 2 : Set $P := (a, b)$, $B := b^2 - a^2 - Aa \pmod N$, $E : y^2 = x^3 + Ax + B$, $j = 1$.
Step 3 : Put $j := j + 1$, $P := jP \in E(\mathbb{Z}/N\mathbb{Z})$. If this fails, let d be the integer (mod N) that could not be inverted (mod N).

Case (i): $d < N$. Output (d, N) and stop.
Case (ii): $d = 0$.[1] Go to Step 1.

Step 4 : Go to Step 3.

Notice that it tries *more than one elliptic curve* E. This gives the flexibility of $|E(\mathbb{F}_p)|, |E(\mathbb{F}_q)|$ that we did *not* have with $|(\mathbb{Z}/p\mathbb{Z})^*|, |(\mathbb{Z}/q\mathbb{Z})^*|$ (always $= p-1, q-1$).

Another (simpler) elliptic curve factoring method is the following PARI functin, which uses idea (2) above:

```
{ECM(N,m) = local(E);
   E = ellinit([0,0,0,random(N),1]*Mod(1,N));
   print(''E: y^2 = x^3 + '', lift(E[4]), ''x+1, P=[0,1]'');
   ellpow(E, [0,1]*Mod(1,N), m)}
```

It works well for 6313 even if m is as small as 100.

By the way, I know the order of $E(\mathbb{F}_{59})$ (for $y^2 = x^3 + x + 54$) not by computing it, but by PARI: after defining $E59$ and $E107$ (using `ellinit`),

```
gp>       ellap(E59,59)
=3
gp>       ellap(E107,107)
=-8
```

computes the a_p satisfying $p + 1 - a_p = |E(\mathbb{F}_p)|$. So $|E(\mathbb{F}_{59})| = 59 + 1 - 3 = 57$ (as claimed) and $|E(\mathbb{F}_{107})| = 107 + 1 + 8 = 116 = 4 \cdot 29$.

Exercises

(1) Use Lenstra's elliptic curve factorization algorithm to factor each of the numbers N using the given elliptic curve E and point P. (Use PARI.)
   (a) $N = 589$, E: $y^2 = x^3 + 4x + 9$, $P = (2, 5)$
   (b) $N = 28102844557$, E: $y^2 = x^3 + 18x - 453$, $P = (7, 4)$.

[1] This means you hit o in $E(\mathbb{F}_p)$ and $E(\mathbb{F}_q)$ simultaneously, roughly speaking.

CHAPTER 28

Pairing-based cryptography

We have so far discussed cryptographic schemes by which two people can arrive at a shared secret key, and by which multiple persons can use a single "receiver's" public key info to send him or her messages. This leaves open the question of how multiple people might arrive at a shared secter key, or of how to construct a network in which anyone can securely send anyone else a message. Let's begin with the first of these.

2-round 3-party key agreement. The principals of the accounting firm **D**ewey, **C**heatham, and **H**owe want to arrive at a shared secret key κ, working over an insecure channel. They need to start by agreeing on a finite cyclic group G with generator γ. (For instance, this might be $G = (\mathbb{F}_p^*, \cdot)$ or the subgroup of some $E(\mathbb{F}_p)$ generated by a point $\gamma = P$.) Next, they pick secret integers d, c, and h respectively. (Really, if $\langle\gamma\rangle \cong \mathbb{Z}/m\mathbb{Z}$, these are elements of $\mathbb{Z}/m\mathbb{Z}$, but if $G \leq E(\mathbb{F}_p)$ they might not know what m is.)

Now they (publicly) send each other the following elements of G:

- Dewey sends Cheatham γ^d;
- Chetham sends Howe γ^c; and
- Howe sends Dewey γ^h.

This is Round 1. Now they look at what they have received, and exponentiate and broadcast again (Round 2):

- Dewey sends Cheatham $(\gamma^h)^d$;
- Cheatham sends Howe $(\gamma^d)^c$; and
- Howe sends Dewey $(\gamma^c)^h$.

Finally each one exponentiates (and does NOT broadcast) what s/he has received one more time, to obtain

$$\underset{\text{D}}{((\gamma^c)^h)^d} = \underset{\text{C}}{((\gamma^h)^d)^c} = \underset{\text{H}}{((\gamma^d)^c)^h},$$

which is κ.

Now the state Attorney General thinks he might be on to a money laundering ring. To get his incriminating evidence, he needs to break their code by determining κ. By tapping their phone line he has overheard G, γ, γ^d, γ^c, γ^h, γ^{hd}, γ^{dc}, and γ^{ch}. So if he can solve the discrete log problem for d, c, h, hd, dc, or ch, he's got 'em. Fortunately they hadn't heard of 1-round 3-party key agreements, which make use of . . .

Bilinear pairings. Given finite cyclic groups G and H of prime order m,[1] a **bilinear pairing** is a map

$$\begin{array}{ccc} G \times G & \to & H \\ (g_1, g_2) & \mapsto & \langle g_1, g_2 \rangle \end{array}$$

satisfying

- **bilinearity**:[2] for all $g_1, g_1', g_2, g_2' \in G$, we have

$$\langle g_1 g_1', g_2 \rangle = \langle g_1, g_2 \rangle \langle g_1', g_2 \rangle$$

  and

$$\langle g_1, g_2 g_2' \rangle = \langle g_1, g_2 \rangle \langle g_1, g_2' \rangle;$$

- **nondegeneracy**: if γ generates G, then $\langle \gamma, \gamma \rangle$ generates H.

Notice that bilinearity $\implies \langle g_1^a, g_2^b \rangle = \langle g_1, g_2 \rangle^{ab}$. Since g_1 and g_2 are powers of γ, this also gives $\langle g_1, g_2 \rangle = \langle g_2, g_1 \rangle$. Preferably, the pairing $\langle\ ,\ \rangle$ should be efficiently computable.

For what follows, we will need to assume that the **bilinear Diffie-Hellman problem** of computing $\langle \gamma, \gamma \rangle^{abc}$ from $\gamma, \gamma^a, \gamma^b, \gamma^c$ is as hard as the usual Diffie-Hellman problem in G and H (computing γ^{ab} from $\gamma, \gamma^a, \gamma^b$).

---

[1] they're the same group abstractly, but will often be presented differently – e.g., $G \leq E(\mathbb{F}_p)$ and H the group of m^{th} roots of unity in $\mathbb{C}$.

[2] the name comes from the appearance of this property if we write the groups additively: $\langle g_1 + g_1', g_2 \rangle = \langle g_1, g_2 \rangle + \langle g_1', g_2 \rangle$, etc.

1-round 3-party key agreement. As before, the partners in the law firm **S**ue, **G**rabbitt and **R**unne agree publicly on G and γ, choose secret integers s, g, r, and broadcast $\gamma^s, \gamma^g, \gamma^r$. Now

- Sue computes $\langle \gamma^g, \gamma^r \rangle^s$
- Grabbitt computes $\langle \gamma^s, \gamma^r \rangle^g$
- Runne computes $\langle \gamma^s, \gamma^g \rangle^r$

and all three of these computations yield $\kappa := \langle \gamma, \gamma \rangle^{sgr}$. A lot less information has been broadcast to arrive at this shared secret than in the 2-round scheme. (Too bad for the AG.)

Hash functions. For the next application of pairings, we need the notion of a cryptographic hash function. Let $\{0,1\}^\ell$ denote the set of bitstrings of length ℓ, and $\{0,1\}^*$ the set of bitstrings of arbitrary length. Begin by chopping up some $D \in \{0,1\}^*$ into substrings of length ℓ (adding zeroes if needed): $D = D_1 D_2 \cdots D_k$. Choose a "mixing" function $M : \{0,1\}^\ell \to \{0,1\}^\ell$ and some $E_0 \in \{0,1\}^\ell$. Then define iteratively $E_i := E_{i-1} \oplus M(D_i)$, where $\oplus$ is binary XOR, and put $\mathcal{H}(D) := E_k$. This defines a function $\mathcal{H} : \{0,1\}^* \to \{0,1\}^\ell$,which is easy to compute and (typically) hard to invert. In practice, the range space "$\{0,1\}^\ell$" might (say) be replaced by a group G, which just means that we compose with a map from $\{0,1\}^\ell \to G$; the same goes for the domain of $\mathcal{H}$.

An ID-based cryptographic network. This is a general mcryptographic scheme, due to Boneh and Franklin, which allows for a large number of participants to send each other messages. It requires a trusted third party Ted, who chooses (and publishes) the groups G and H, the pairing $\langle\ ,\ \rangle : G \times G \to H$, a generator $g \in G$, as well as hash functions $\mathcal{H}_1 : \{0,1\}^* \to G$ and $\mathcal{H}_2 : H \to \{0,1\}^\mu$ (where $\{0,1\}^\mu$ is the set of possible plaintext messages). ted also chooses a secret integer s and publishes $\mathcal{K} = g^s \in G$, the *master public key*.

Each member of the network has an ID $\in \{0,1\}^*$, which is publicly available (e.g., e-mail addresses). Each ID gives rise to a public key κ (which anyone can compute) and a private key σ (which only

Ted can compute), both in G. For instance, from Alice's ID_A we have $\kappa_A := \mathcal{H}_1(\mathrm{ID}_A)$ and (red has) $= (\mathcal{H}_1(\mathrm{ID}_A))^s$.

Now suppose Bob has a message $\mathcal{M} \in \{0,1\}^\mu$ for Alice. He chooses an ephemeral key ε (= random integer), then computes and broadcasts the ciphertext

$$(c_1, c_2) := (g^\varepsilon, \mathcal{M} \oplus \mathcal{H}_2(\langle \kappa_A, \mathcal{K}\rangle^\varepsilon)) .$$

Alice now uses her private key (which was securely sent to her by Ted) to decrypt:

$$\begin{aligned} c_2 \oplus \mathcal{H}_2\left(\langle \sigma_A, c_1\rangle\right) &= \mathcal{M} \oplus \mathcal{H}_2(\langle \kappa_A, \mathcal{K}\rangle^\varepsilon) \oplus \mathcal{H}_2(\langle \sigma_A, g^\varepsilon\rangle) \\ &= \mathcal{M} \oplus \mathcal{H}_2(\langle \kappa_A, g^s\rangle^\varepsilon) \oplus \mathcal{H}_2(\langle \kappa_A^s, g^\varepsilon\rangle) \\ &= \mathcal{M} \end{aligned}$$

since $\langle \kappa_A, g^s\rangle^\varepsilon = \langle \kappa_A, g\rangle^{s\varepsilon} = \langle \kappa_A^s, g^\varepsilon\rangle$.

Without getting into *how* Ted would securely deliver σ_A to Alice, the more interesting question is "when": for example, maybe Ted gives all the secret keys $\sigma_{\cdots}$ to their owners at the beginning of this exercise; maybe they have to request them; or *maybe* they have to satisfy some condition to receive it (payment, minimum age, expiry date, etc.). In the latter case, how would Chris send Alice a message with no such conditions? The solution is for the different senders to "enrich" ID_A by adding (say) their own name, conditions for receipt, etc. and publishing this sender-and-message-specific ID'_A. Ted then sends the corresponding σ'_A to Alice for each message, as she meets these conditions for receipt.

Naturally, we should ask whether this scheme is secure. Ivan the Interceptor sees (c_1, c_2), but to recover $\mathcal{M}$ from that he'd have to compute $\langle \kappa_A, \mathcal{K}\rangle^\varepsilon$; if we write κ_A as g^α, then this is $\langle g^\alpha, g^s\rangle^\varepsilon = \langle g, g\rangle^{\alpha s\varepsilon}$. Ivan knows g, $c_1 = g^\varepsilon$, $\kappa_A = g^\alpha$, and $\mathcal{K} = g^s$, so this is precisely the bilinear Diffie-Hellman.

The attentive reader will likely have remarked that this all sounds quite glorious, but without an actual pairing will be about as useful

as a wooden frying pan. That, and it has nothing to do with elliptic curves. Right?

CHAPTER 29

Divisors and the Weil pairing

It turns out that elliptic curves of a certain kind are actually the key to constructing useful "bilinear pairings" in the sense of the last section. The setup for this construction will require a brief tour of results whose proofs are a bit beyond the scope of this course.[1] We begin by describing the "divisor class group" of an elliptic curve, which is a geometric analogue of the "ideal class groups" of number rings that we'll explore in the last segment of these notes.

Divisors. Let K be a field (for our purposes, $K \subset \mathbb{C}$ or $K = \mathbb{F}_{p^k}$), E: $y^2 = x^3 + Ax + B$ an elliptic curve (with $A, B \in K$, $4A^3 + 27B^2 \neq 0$). Given $R(x,y)$, $S(x,y)$ polynomials with coefficients in K, we may consider the **rational function**

$$f := \left.\frac{R}{S}\right|_E$$

on E; the set of all such forms a field denoted by $K(E)$.

If $R = 0$ and $S = 0$ define curves C_R and C_S in the xy-plane, then f has zeroes where C_R meets E and poles ($= \infty$) where C_S meets E; f can also have a zero or pole at o, the point at infinity. As in our discussion of lines meeting E, we asssign (integer) multiplicities to each zero and pole (e.g., ≥ 2 if C_R is tangent to E). The idea is that if z is a "local coordinate on E" at a point P, vanishing at P, then $f \sim$ const. $\times z^{n_P(f)}$ there for some integer $n_P(f)$ (> 0 for a zero, < 0 for a pole).

[1] In particular, this material won't appear on the final. On the other hand, if you are interested in more details, J. Silverman's book "The Arithmetic of Elliptic Curves" contains proofs, as does the excellent article "The Weil pairing, and its efficient calculation" by V. Miller. (I've also put a few hints in the footnotes, which can be skipped.)

A **divisor** on E is a finite formal sum

$$\sum n_P[P] \qquad (n_P \in \mathbb{Z})$$

of points $P \in E(K)$.[2] They form a group $Div(E)$, with a **degree map**

$$\begin{array}{rccc} \deg: & Div(E) & \to & \mathbb{Z} \\ & \sum n_P[P] & \mapsto & \sum n_P \end{array}$$

whose kernel (the stuff mapping to zero) is the subgroup $Div^0(E)$ of divisors of degree 0.

The divisor of a (nonzero) function $f \in K(E)^*$ is the formal sum

$$(f) := \sum_{P \in E(\bar{K})} n_P(f)[P];$$

these always have degree zero.[3] Moreover, we have $(fg) = (f) + (g)$, $(\frac{1}{f}) = -(f)$, and $(\text{const.}) = 0$. So the set $PDiv(E)$ of **principal divisors**, or divisors of rational functions on E, is a subgroup of $Div^0(E)$. Taking quotients gives the divisor class groups

$$\underbrace{\frac{Div^0(E)}{PDiv(E)}}_{=:Cl^0(E)} \hookrightarrow \underbrace{\frac{Div(E)}{PDiv(E)}}_{=:Cl(E)} \overset{\deg}{\twoheadrightarrow} \mathbb{Z},$$

---

[2] Technically, we must also allow sums of points in $E(\bar{K})$ ($\bar{K}$ = algebraic closure of K) which are defined by polynomial equations over K. So if we were working on a line over (say) $K = \mathbb{R}$, we would have to allow (for example) $[i] + [-i]$ since this is defined by $x^2 + 1 = 0$.

[3] Recall the notion of projective plane $\mathbb{P}^2$(= $\{xy\text{-plane}\} \cup \{\text{line at } \infty\}$) consisting of lines through the origin in 3-space, with homogeneous coordinates $[X : Y : Z]$. (E has equation $Y^2Z = X^3 + AXZ + BZ^3$, and $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.) Any rational function $f = \frac{R}{S}|_E$ can be written as a quotient of *homogeneous polynomials* $\frac{\mathcal{R}(X,Y,Z)}{\mathcal{S}(X,Y,Z)}$ of the same degree d – that is, of the form $\sum_{i+j+k=d} a_{ijk}X^iY^jZ^k$. Then writing $(C \cdot E)_P$ for the *intersection multiplicity* of C and E at P, $\sum n_P(f) = \sum_{P \in C_R \cap E}(C_R \cdot E)_P - \sum_{P \in C_S \cap E}(C_S \cdot E)_P = d - d = 0$, as claimed.

Alternatively, one could (working over $\mathbb{C}$) cut open E as in §IV.F and integrate around the boundary; by residue theory (complex analysis) $0 = \frac{1}{2\pi i} \oint \frac{df}{f} = \sum n_P(f)$.

and **Abel's Theorem** says that the map

$$\begin{array}{ccc} Cl^0(E) & \stackrel{\Phi}{\to} & E(K) \\ \sum\limits_{\text{(formal)}} n_P[P] & \mapsto & \sum n_P P \end{array}$$

(where the right-hand side is the sum in the group law on E) is an isomorphism of groups:

THEOREM 221. *$\sum n_P[P] \in Div(E)$ is the divisor of a function $f \in K(E)$ if and only if*[4] *$\sum n_P P = o$ in the group law on $E(K)$.*

EXAMPLE 222. Suppose $P, Q \in E(K)$, and let $\ell_{PQ}(x,y) = 0$ be the (linear) equation defining L_{PQ}, the line through P and Q. Then writing

$$f_{PQ} := \left.\frac{\ell_{PQ}}{\ell_{P*Q,o}}\right|_E \in K(E)^*,$$

we have

$$(f_{PQ}) = [P] + [Q] - [P+Q] - [o].$$

This yields the "if" part in Theorem 221, since any divisor $D = \sum n_P[P]$ with $\sum n_P = 0$ and $\sum n_P P = o$ can be written $D = \sum n_{PQ}([P] + [Q] - [P+Q] - [o])$.

EXAMPLE 223. Assume $x^3 + Ax + B = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ and $y^2 - B = (y+\beta)(y-\beta)$; let $P_i = (\alpha_i, 0)$, $\pm Q = (0, \pm\beta)$. Then viewing x, y as functions on E,[5]

$$(x) = [Q] + [-Q] - 2[o]$$

[4]The "only if" part is most easily seen (over $\mathbb{C}$) by cutting open E and integrating $0 = \oint u\frac{df}{f}$ where (in the $\mathbb{C}/\Lambda$ model of $E(\mathbb{C})$) u is the coordinate on $\mathbb{C}$.

[5]To compute the multiplicities at ∞, write the functions and the equation of E in homogeneous coordinates:

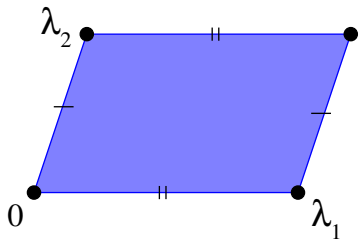
$$-Y^2Z + X^3 + AXZ^2 + BZ^3 = 0, \quad X/Z, \quad Y/Z.$$

At $o = [0:1:0]$, Y doesn't vanish; while restricting E's equation to $X = 0$ resp. $Z = 0$ yields $Z(BZ^2 - Y^2) = 0$ resp. $X^3 = 0$ ($\Longrightarrow$ intersection multiplicities 1 resp. 3 at o). So $n_o(x) = n_o(X/Z) = 1 - 3 = -2$ while $n_o(y) = n_o(Y/Z) = -3$.

and

$$(y) = [P_1] + [P_2] + [P_3] - 3[o].$$

Torsion points. Recall the model of $E(\mathbb{C})$ as $\mathbb{C}/\Lambda$, with $\Lambda \cong \mathbb{Z}\langle\lambda_1, \lambda_2\rangle$ the lattice generated by two complex numbers with ratio $\frac{\lambda_2}{\lambda_1} \notin \mathbb{R}$:

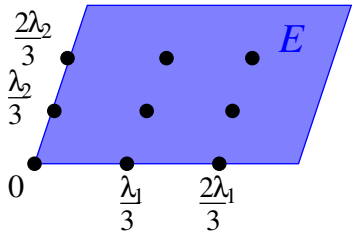


We are interested in the set of points of a given order in the group law:

DEFINITION 224. Given $m \in \mathbb{N}$, the **m-torsion subgroup** of $E(K)$ is

$$E(K)[m] := \{P \in E(K) \mid mP = o\}.$$

From the picture (with $m = 3$)



we "see" that (for all m)

$$E(\mathbb{C})[m] \cong \tfrac{1}{m}\Lambda/\Lambda \cong \mathbb{Z}_m \times \mathbb{Z}_m.$$

(Notice that if m is prime, then this is a 2-dimensional vector space over $\mathbb{F}_m$.)

In cryptography, we are interested not in $K = \mathbb{C}$ but $K = \mathbb{F}_p$ or more generally $\mathbb{F}_p^k$. For any p, m (with $p \nmid m$) one can in fact show that

$$E(\mathbb{F}_{p^k})[m] \leq \mathbb{Z}_m \times \mathbb{Z}_m \tag{52}$$

with equality for $k \geq k_0$ sufficiently large. (This k_0 is called the **embedding degree**.)

EXAMPLE 225. Let E be given by $y^2 = x^3 - x$, and p be any odd prime. Then

$$E(\mathbb{F}_p)[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

consists of $(1,0)$, $(0,0)$, $(-1,0)$, and o.

EXAMPLE 226. We stick with the same equation $y^2 = x^3 - x$. Let p, ℓ be distinct primes such that there exists $P \in E(\mathbb{F}_p)[\ell] \backslash \{o\}$; clearly $\langle P \rangle$ is then a cyclic subgroup of order ℓ. When does there exist a $Q \in E(\mathbb{F}_p)[\ell] \backslash \langle P \rangle$? (Notice that this would guarantee $E(\mathbb{F}_p)[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.)

One could try to look for an automorphism (that is, a self-map which is invertible and a group homomorphism) ϕ of E that would send P to another ℓ-torsion point. If $p \underset{(4)}{\equiv} 1$ then there is an $\alpha \in \mathbb{F}_p$ with $\alpha^2 = -1$, and $\phi(x,y) := (-x, \alpha y)$ gives such a map. But we might have $\phi(P) \in \langle P \rangle$, which defeats the purpose.

To avoid this possibility, suppose instead that $p \underset{(4)}{\equiv} 3$. Then it turns out that while -1 is not a square in $\mathbb{F}_p$, it *is* a square[6] in $\mathbb{F}_{p^2}$. Then $\phi(P)$ won't be in $E(\mathbb{F}_p)$ but in $E(\mathbb{F}_{p^2})[\ell] \backslash E(\mathbb{F}_p)[\ell]$, so can't possibly be a multiple of P; and $E(\mathbb{F}_{p^2})[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ is generated by P and $Q := \phi(P)$. For this reason, it is easier to construct examples where equality holds in (52) if we allow fields of prime *power* order.

EXAMPLE 227. Same E, $p = 11$, $P = (4,4) \in E(\mathbb{F}_{11})[3] \implies Q = \phi(P) = (-4, 4\alpha) \in E(\mathbb{F}_{11^2})[3]$.

[6]Recall that $\mathbb{F}_{p^k}$ can be constructed by taking the quotient of the polynomial ring $\mathbb{F}_p[t]$ by the ideal generated by an irreducible polynomial of degree k. If $p \underset{(4)}{\equiv} 3$ then -1 is not a square mod p, and so $t^2 + 1$ is irreducible in $\mathbb{F}_p[t]$. So $\mathbb{F}_{p^2} \cong \mathbb{F}_p[t]/(t^2+1)$ means that we may think of $\mathbb{F}_{p^2}$ as $\mathbb{F}_p + \alpha \mathbb{F}_p$, where $\alpha^2 = -1$.

The **support** of a divisor $D = \sum n_P[P]$ is just the union of all the points P appearing (with $n_P \neq 0$). If we write $Div^{(0)}(E)[m]$ for the (degree 0) divisors supported on m-torsion, then the group of corresponding divisor classes is

$$Cl^0(E)[m] \underset{\Phi}{\overset{\cong}{\rightarrow}} E(K)[m]. \tag{53}$$

The Weil pairing. We shall use the following convention for "evaluating" a function $f \in K(E)$ on a divisor $D = \sum n_P[P] \in Div(E)$:

$$f(D) := \prod_P f(P)^{n_P} \in K.$$

(Note that this only makes sense if the supports of D and (f) are disjoint.) If (f) and (g) have disjoint supports, a basic result (which we will not prove) is **Weil reciprocity**:

$$f((g)) = g((f)).$$

Given $D_1, D_2 \in Div^0(E)[m]$, $\Phi(D_i)$ is m-torsion, so $\Phi(mD_i) = o$ and mD_i is the divisor of a function $f_i \in K(E)$. Suppose the supports of D_1 and D_2 are disjoint, so that

$$\langle D_1, D_2 \rangle := \frac{f_1(D_2)}{f_2(D_1)} \in K^* \tag{54}$$

makes sense. This has the following properties:

- $\langle D_1, D_2 \rangle$ belongs to the subgroup $\mu_m(K) \leq K^*$ of m^{th} roots of unity, since $\langle D_1, D_2 \rangle^m = \frac{f_1(D_2)^m}{f_2(D_1)^m} = \frac{f_1(mD_2)}{f_2(mD_1)} = \frac{f_1((f_2))}{f_2((f_1))} = 1$ by Weil reciprocity.
- $\langle\ ,\ \rangle$ depends only on the divisor *classes* (in $Cl^0(E)[m] \cong E(K)[m]$), since[7] if (say) $D_1 = (f)$ then $f_1 = f^m$ and $\frac{f_1(D_2)}{f_2(D_1)} = \frac{f(D_2)^m}{f_2((f))} = \frac{f((f_2))}{f_2((f))} = 1$ (again by Weil).
- $\langle\ ,\ \rangle$ is "antisymmetric" in the sense that $\langle D_1, D_2 \rangle = \langle D_2, D_1 \rangle^{-1}$, and "bilinear" in the sense that $\langle D_1 + D_1', D_2 \rangle = \langle D_1, D_2 \rangle \langle D_1', D_2 \rangle$ etc. (easy exercise).

[7] Also, multiplying f_1 and f_2 by a constant doesn't matter since they are being evaluated on divisors of degree *zero*.

The **Weil pairing** is the bilinear map

$$(\ , \ ) : \ E(K)[m] \times E(K)[m] \to \mu_m(K)$$

induced by (54). To compute it on $P, Q \in E(K)[m]$, we can take $D_P = [P] - [o]$, $D_Q = [Q] - [o]$ and the corresponding $f_P, f_Q \in K(E)$; but D_P and D_Q don't have disjoint support. To fix this, put $\tilde{D}_Q = [Q + S] - [S]$ for some arbitrary $S \in E(K)\backslash\{o, P, -Q, P - Q\}$, with corresponding $\tilde{f}_Q$; then $\Phi(D_P) = P$, $\Phi(\tilde{D}_Q) = Q \implies$

$$(P, Q) = \langle D_P, \tilde{D}_Q \rangle = \frac{f_P(\tilde{D}_Q)}{\tilde{f}_Q(D_P)} = \frac{f_P(Q+S)/f_P(S)}{\tilde{f}_Q(P)/\tilde{f}_Q(o)}$$

$$= \frac{f_P(Q+S)/f_P(S)}{f_Q(P-S)/f_Q(-S)}.$$

We remark that if $2 \nmid m$, antisymmetry $\implies (P, P) = 1$ for any P. (Why?)

What makes the Weil pairing useful is the key property of *nondegeneracy*:

- If $P \neq o$ and $Q \notin \langle P \rangle$, then $(P, Q) \neq 1$. (If m is prime, this means that (P, Q) is a primitive m^{th} root of 1.)

For simplicity we shall assume from now on that that m is prime. So in particular, there exist P and Q with $(P, Q) \neq 1$ if and only if $E(K)[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$, in which case they form a basis of $E(K)[m]$. From this point of view, the Weil pairing is rather like a 2×2 determinant since for an arbitrary pair of elements in $E(K)[m]$, we have

$$(a_{11}P + a_{12}Q, a_{21}P + a_{22}Q) =$$

$$= (P, P)^{a_{11}a_{21}} (Q, Q)^{a_{12}a_{22}} (P, Q)^{a_{11}a_{22}} (Q, P)^{a_{12}a_{21}}$$

$$= (P, Q)^{a_{11}a_{22} - a_{12}a_{21}} = (P, Q)^{\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}.$$

We shall only give the simplest example of a computation of the Weil pairing, but a "double-and-add" algorithm for computing it efficiently has been devised by Miller.

EXAMPLE 228. Once more let E be given by $y^2 = x^3 - x = x(x+1)(x-1)$, p be any odd prime, and $K = \mathbb{F}_p$ (or $\mathbb{F}_{p^k}$). Consider the 2-torsion points $P_1 = (1,0)$, $P_2 = (0,0)$, $P_3 = (-1,0)$, so that $f_{P_1} = x-1$, $f_{P_2} = x$, $f_{P_3} = x+1$ have divisors $(f_i) = 2[P_i] - 2[o]$. Then (writing $S = (x_0, y_0)$)

$$x(P_1 - S) = \left(\frac{-y_0}{x_0 - 1}\right)^2 - x_0 - 1 = \frac{x_0 + 1}{x_0 - 1}$$

$$x(P_3 + S) = \left(\frac{y_0}{x_0 + 1}\right)^2 - x_0 - (-1) = \frac{1 - x_0}{1 + x_0}$$

$$(P_1, P_3) = \frac{f_{P_1}(P_3 + S) f_{P_3}(-S)}{f_{P_1}(S) f_{P_3}(P_1 - S)} = \frac{(x(P_3 + S) - 1)(x_0 + 1)}{(x_0 - 1)(x(P_1 - S) + 1)}$$

$$= \frac{1 - x_0 - (x_0 + 1)}{x_0 + 1 + (x_0 - 1)} = \frac{-2x_0}{2x_0} = -1.$$

This demonstrates the nondegeneracy of Weil on 2-torsion.

Applications. Suppose that $E(\mathbb{F}_p)[m] \cong \mathbb{Z}_m$, with generator P. Let k be the corresponding embedding degree,[8] so that $E(\mathbb{F}_{p^k})[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$, with generators P and Q. Since the Weil pairing is a map from $E(\mathbb{F}_{p^k})[m] \times E(\mathbb{F}_{p^k})[m] \to \mu_m \leq \mathbb{F}_{p^k}^*$, taking the pairing with Q gives an isomorphism

$$\Psi : \langle P \rangle = E(\mathbb{F}_p)[m] \xrightarrow{\cong} \mu_m = \langle (P, Q) \rangle \leq \mathbb{F}_{p^k}^*.$$

Given $R \in \langle P \rangle$, we can solve an instance of the ECDLP (compute $\log_P R$) in $E(\mathbb{F}_p)$ by solving the corresponding DLP (that is, computing $\log_{(P,Q)}(R, Q)$) in $\mathbb{F}_{p^k}^*$. The latter can be done in subexponential time, via the index calculus (see §V.A). This is the idea behind the Menezes-Okamoto-Vanstone (MOV) algorithm for the ECDLP.

But doesn't this contradict our earlier assertion that, in general, there are only exponential-time algorithms for ECDLP? Actually, it

[8] which depends on p and m

doesn't: the embedding degree k is usually very large, and "subexponential time" in p^k worse than "exponential time" in $|E(\mathbb{F}_p)|$. However, the above "MOV attack" may persuade us to steer clear of using elliptic curves with small embedding degree for ECDLP-based cryptosystems like elliptic El Gamal.

On the other hand, such curves are *exactly what we need* if we want to do pairing-based cryptography! A case in point is the class of *supersingular elliptic curves* with $|E(\mathbb{F}_p)| = p + 1$, for which the embedding degree is often 2, as was demonstrated in Example 226 for the curve $y^2 = x^3 - x$ with $p \underset{(4)}{\equiv} 3$. There's only one problem: the Weil pairing is not a pairing in the sense of §V.D, since $(P, P) = 1$.

To fix this, recall the self-map $\phi : E(\mathbb{F}_{p^k})[m] \to E(\mathbb{F}_{p^k})[m]$ from that Example, sending $P \mapsto Q = \phi(P)$. We can define a bilinear pairing in the sense of §V.D

$$\langle P \rangle \times \langle P \rangle \to \langle (P, Q) \rangle$$

by $\ll R_1, R_2 \gg := (R_1, \phi(R_2))$. (Supersingular curves always have self-maps of this sort.) So now we see that elliptic curves (and the Weil pairing) really are the ticket to actualize the pairing-based cryptosystems described there.

Exercises

(1) Verify that the Weil pairing is antisymmetric, bilinear, and that $(P, P) = 1$. (This should take no more than 3 lines. If you want a more challenging "check", try [HPS] #5.27(b).)
(2) Compute the Weil pairing on the points P and Q of Example V.E.7. (You could do it "by hand" or look up Miller algorithm in [HPS] and use that.)

Part 6

Algebraic numbers

CHAPTER 30

Algebraic number fields

As we saw in our study of quadratic Diophantine equations, to better understand integral solutions it was helpful to think about *nonintegers* – in particular, those involving square roots, and the properties of *quadratic number rings* built fom these numbers. More general algebraic number rings and fields play a similar role in the study of Diophantine equations of degree greater than two. They also are deeply intertwined with hyperbolic geometry, algebraic geometry, representation theory, and many other areas of mathematics. While we'll only skim the surface of algebraic number theory in what follows, we'll at least learn enough to see a beautiful application to Fermat's Last Theorem.

Given $K \subseteq L$ fields, L is a vector space over K; we denote its dimension by $[L : K]$, and call L/K a **field extension** of **degree** $[L : K]$.

Given $K \subseteq L \subseteq M$ fields, with $\{\ell_1, \ldots, \ell_d\} \subset L$ a basis of L/K, and $\{m_1, \ldots, m_e\} \subset M$ a basis of M/L, $\{\ell_i m_j\}_{i,j} \subset M$ is a basis of M/K. Since there are $d \cdot e$ elements in this basis, we conclude the **tower law**

$$[M : K] = [M : L][L : K].$$

DEFINITION 229. We say that an element $\alpha \in L$ is **algebraic** over K iff $f(\alpha) = 0$ for some polynomial $f \in K[X]$; and that L/K is an **algebraic field extension** iff *all* elements of L are algebraic over K.

If $[L : K] =: d$ is finite, then for any $\alpha \in L$, $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ are dependent over K. Hence there exists $f \in K[X]$ of degree $\leq d$ such that $f(\alpha) = 0$. It follows that a field extension of finite degree is always algebraic. (The converse isn't true, as we're about to see.)

DEFINITION 230. A number $\alpha \in \mathbb{C}$ which is algebraic over $\mathbb{Q}$ is called an **algebraic number**. The set of all such is denoted $\bar{\mathbb{Q}}$.

THEOREM 231. *$\bar{\mathbb{Q}}$ is a field.*

PROOF. Given $\alpha, \beta \in \bar{\mathbb{Q}}$, we show $\alpha\beta$, $\alpha + \beta$, $\alpha^{-1} \in \bar{\mathbb{Q}}$. Say $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$ and $\beta^m + s_1\beta^{m-1} + \cdots + s_m = 0$, where $r_i, s_j \in \mathbb{Q}$ and $r_n \neq 0$. Then span $\left(\{\alpha^i\beta^j\}_{\substack{0 \le i < n \\ 0 \le j < m}} \right)$ is closed under multiplication by α, β, hence by $\alpha + \beta$, $\alpha\beta$ (which it contains) $\implies$ $\alpha + \beta$, $\alpha\beta$ satisfy equations of degree $\le nm$. As for α^{-1}, we have $\alpha^{-1} = -r_n^{-1}(\alpha^{n-1} + r_1\alpha^{n-2} + \cdots + r_{n-1})$. □

In particular, we see that polynomials $\mathbb{Q}[\alpha]$ in α are the same as rational functions $\mathbb{Q}(\alpha)$ in α.

DEFINITION 232. A field K with $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ and $[K : \mathbb{Q}] < \infty$ is called an **algebraic number field**. (Clearly $\mathbb{Q}(\alpha)$ is an example, for any algebraic number α.)

Now consider an ideal $I \subset k[X]$, k any field. Then $I \backslash \{0\}$ has an element g of least degree. If $f \in I \backslash \{0\}$ is arbitrary, polynomial division $\implies$ $f = gq + r$, $\deg r < \deg g$ $\implies$ $r = f - gq \in I$, contradicting minimality of $\deg g$ unless $r = 0$. So $f = gq \in (g)$. Since f was arbitrary, $I = (g)$.

THEOREM 233. *Any ideal in $k[X]$ is principal; we say that $k[X]$ is a **PID** (**principal ideal domain**).*

Given a ring R containing k, and $\alpha \in R$, consider the ring homomorphism

$$\begin{array}{rccc} \phi_\alpha : & k[X] & \to & R \\ & f(X) & \mapsto & f(\alpha). \end{array} \tag{55}$$

Since $\phi_\alpha(f) = 0 \implies \phi_\alpha(fg) = \phi_\alpha(f)\phi_\alpha(g) = 0$, $\ker(\phi_\alpha)$ is an ideal. By Theorem 233, $\ker(\phi_\alpha) = (m_\alpha)$ for some $m_\alpha \in k[X]$, where we may assume m_α is **monic** (i.e. its leading coefficient is 1).

DEFINITION 234. (i) m_α is called the **minimal polynomial** of α over k. (Clearly, it is the polynomial of least degree with coefficients in k and having α as a root.)

(ii) The **degree** of an algebraic number α (over $\mathbb{Q}$) is $\deg(m_\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. (A basis of $\mathbb{Q}(\alpha)$ is $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(m_\alpha)-1}\}$.)

PROPOSITION 235. *The minimal polynomial of an algebraic number is irreducible and has no repeated roots.*

PROOF. If $m_\alpha = fg$ (both factors nonconstant), then $0 = m_\alpha(\alpha) = f(\alpha)g(\alpha)$; by minimality, neither $f(\alpha)$ nor $g(\alpha)$ can be 0, a contradiction. So m_α is irreducible over $\mathbb{Q}$. Write m'_α for its (formal) derivative.

Next, $\deg m'_\alpha < \deg m_\alpha$ and irreducibility of $m_\alpha \implies m'_\alpha, m_\alpha$ have no common factor in $\mathbb{Q}[X] \implies (m'_\alpha, m_\alpha) = (1) = \mathbb{Q}[X] \implies \exists\, f, g \in \mathbb{Q}[X]$ such that

$$fm'_\alpha + gm_\alpha = 1. \tag{56}$$

If over $\mathbb{C}$ $m_\alpha = (x-\rho)^2 h$, then $(x-\rho) \mid m'_\alpha$ and plugging ρ into (56) gives $0 = 1$, a contradiction. So there are no repeated roots. □

THEOREM 236 (**Theorem of the Primitive Element**). *Every algebraic number field K has the form $K = \mathbb{Q}(\theta)$, $\theta \in K$. (It is this element θ that is called the primitive element.) That is, every element in K is of the form $\sum_{j=0}^{[K:\mathbb{Q}]} q_j \theta^j$, $q_j \in \mathbb{Q}$.*

IDEA OF PROOF. *A priori* we have $K = \mathbb{Q}(\theta_1, \theta_2, \ldots, \theta_m)$; reduce the number of generators by showing θ_1, θ_2 can be replaced by $\theta_1 + \lambda\theta_2$ ($\lambda \in \mathbb{Q}$), etc. □

EXAMPLE 237. $(\mathbb{Q}(\sqrt{3}))(\sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3}+\sqrt{2})$. Since the left-hand side has degree 4 (over $\mathbb{Q}$) by the tower law, it suffices to show that $\deg(m_{\sqrt{3}+\sqrt{2}}) > 2$. (Degree 3 is impossible, again by the tower law; so then degree 4 is forced, and with it, the equality.) This is easy since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are independent over $\mathbb{Q}$.

Let K have primitive element θ, and $End_{\mathbb{Q}}(K)$ denote the ring of $\mathbb{Q}$-linear transformations ("endomorphisms") from K to K. Clearly

$n := \deg(m_\theta) = [K : \mathbb{Q}]$. Considering the map (55) in this setting

$$\begin{array}{ccccc} \mathbb{Q}[X] & \overset{\phi_\theta}{\twoheadrightarrow} & K & \hookrightarrow & End_{\mathbb{Q}}(K) \\ f(X) & \mapsto & f(\theta) & & \\ & & \kappa & \mapsto & \mu_\kappa \end{array}$$

(μ_κ = multiplication by κ), we find that m_θ is the minimal polynomial of a *matrix* of μ_θ (with respect to any basis of $K/\mathbb{Q}$), hence (by linear algebra) the characteristic polynomial of this matrix:

$$m_\theta(\lambda) = p_\theta(\lambda) := \det(\lambda I - \mu_\theta).$$

Since m_θ has distinct roots, μ_θ diagonalizes over $\mathbb{C}$ with distinct eigenvalues θ_i, one of which (say θ_1) is θ. It follows that, for an arbitrary element $\alpha = \sum_j a_j\theta^j \in K$ ($a_j \in \mathbb{Q}$), μ_α has eigenvalues $\sum_j a_j\theta_i^j =: \sigma_i(\alpha) \in \mathbb{C}$ ($i = 1, \ldots, n$); that is, p_α has roots $\{\sigma_i(\alpha)\}$. Here, $\sigma_1(\alpha) = \alpha$ and the other $\{\sigma_i(\alpha)\}$ are its **Galois conjugates**.

THEOREM 238. *There are $n = [K : \mathbb{Q}]$ distinct field embeddings*

$$\sigma_i : K \hookrightarrow \mathbb{C},$$

and $p_\alpha(\lambda) = \prod_{i=1}^{[K:\mathbb{Q}]}(\lambda - \sigma_i(\alpha)) = (m_\alpha(\lambda))^{\frac{n}{\deg(\alpha)}}$ for any $\alpha \in K$.

PROOF. It is easy to check that the σ_i above are injective homomorphisms from K into $\mathbb{C}$. They are distinct because the $\sigma_i(\theta)$ are. There can't be any more, because given $\sigma : K \hookrightarrow \mathbb{C}$, $0 = \sigma(0) = \sigma(p_\theta(\theta)) = p_\theta(\sigma(\theta)) \implies \sigma(\theta)$ is a root of p_θ (which then determines σ). Finally, $m_\alpha(\alpha) = 0 \implies 0 = \sigma_i(m_\alpha(\alpha)) = m_\alpha(\sigma_i(\alpha)) \implies (\lambda - \sigma_i(\alpha)) \mid m_\alpha(\lambda)$ $(\forall i)$. If $\{\xi_\ell\}$ is the list of *distinct* $\sigma_i(\alpha)$'s, then $\prod(\lambda - \xi_\ell) \mid m_\alpha(\lambda)$. Since $m_\alpha \mid p_\alpha$, these are the only possible roots; and since m_α is irreducible, repeated roots are impossible. So $m_\alpha(\lambda) = \prod_\ell(\lambda - \xi_\ell) \implies p_\alpha \mid m_\alpha^n \implies p_\alpha g = m_\alpha^n \underset{m_\alpha \text{ irred.}}{\implies} p_\alpha = m_\alpha^r$. Now compare degrees. □

EXAMPLE 239. (i) $\mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{C}$ via $a + b\sqrt{d} \mapsto a + b\sqrt{d}, a - b\sqrt{d}$.

(ii) Writing ζ_5 for a primitive 5^{th} root of 1 ($m_{\zeta_5} = X^4 + X^3 + X^2 + X + 1$), $\mathbb{Q}(\zeta_5) \hookrightarrow \mathbb{C}$ via $\zeta_5 \mapsto e^{\frac{2\pi ik}{5}}$, $k = 1, 2, 3, 4$.

Let's look a little more closely at multiplication by $\alpha \in K$ as a $\mathbb{Q}$-linear transformation on K. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $K/\mathbb{Q}$; then (for each i)

$$\alpha\alpha_i = \sum_j a_{ij}\alpha_j,$$

where the $a_{ij} \in \mathbb{Q}$ are the entries of the matrix of μ_α.

DEFINITION 240. (i) $N_{K/\mathbb{Q}}(\alpha) := \det(a_{ij})$ (**norm**).
(ii) $Tr_{K/\mathbb{Q}}(\alpha) := \mathrm{tr}(a_{ij}) = \sum_i a_{ii}$ (**trace**).

Since $\mu_{\alpha\beta} = \mu_\alpha\mu_\beta$ and $\mu_{\alpha+\beta} = \mu_\alpha + \mu_\beta$, $N(\alpha\beta) = N(\alpha)N(\beta)$ and $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$. In the exercises, you will check that the norm and trace of α are independent of the choice of basis. Changing basis so as to diagonalize μ_α, we find:

PROPOSITION 241. *$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$.*

EXAMPLE 242. Viewing $q \in \mathbb{Q}$ as an element of K, we have $N_{K/\mathbb{Q}}(q) = q^n$ and $Tr_{K/\mathbb{Q}}(q) = nq$.

EXAMPLE 243. $K = \mathbb{Q}(\sqrt{d})$ has basis $1, \sqrt{d}$ over $\mathbb{Q}$. Writing $\alpha = a + b\sqrt{d}$, we have $\alpha\sqrt{d} = bd + a\sqrt{d}$ hence

$$[\mu_\alpha] = \begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

which yields $N(\alpha) = a^2 - b^2d$ (which should look familiar) and $Tr(\alpha) = 2a$.

EXAMPLE 244. $K = \mathbb{Q}(\theta)$, where $m_\theta(X) = X^3 - X + 2$. (That is, $\theta^3 = \theta - 2$.) We can use the basis $1, \theta, \theta^2$, and write (for an arbitrary $\alpha \in K$) $\alpha = a + b\theta + c\theta^2$, $\alpha\theta = -2c + (a + c)\theta + b\theta^2$, and $\alpha\theta^2 = -2b + (b - 2c)\theta + (a + c)\theta^2$. This gives

$$[\mu_\alpha] = \begin{pmatrix} a & -2c & -2b \\ b & a + c & b - 2c \\ c & b & a + c \end{pmatrix}$$

and thus the general formulas

$$N(\alpha) = a^3 - 2b^3 + 4c^3 + 2a^2c + ac^2 - ab^2 + 2bc^2 + 6abc$$

and

$$Tr(\alpha) = 3a + 2c.$$

Exercises

(1) Show that $N_{K./\mathbb{Q}}$ and $Tr_{K/\mathbb{Q}}$ are independent of the choice of basis for K as a vector space over $\mathbb{Q}$.
(2) Let $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt[3]{2}$. What are m_θ and $[K : \mathbb{Q}]$? What are the conjugates of θ, i.e. the other roots of m_θ?

CHAPTER 31

Discriminants and algebraic integers

Given the importance of the integers (and rings of quadratic integers like $\mathbb{Z}[\sqrt{d}]$) in this course so far, one might ask: what is the analogue of $\mathbb{Z} \subset \mathbb{Q}$ for general algebraic number fields?

DEFINITION 245. An **algebraic integer** is a number $\alpha \in \mathbb{C}$ that satisfies a *monic* polynomial equation with *integer* coefficients:

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathbb{Z}.$$

The set of all such is denoted by $\bar{\mathbb{Z}}(\subset \bar{\mathbb{Q}})$. Define, for any algebraic number field K, $\mathcal{O}_K := K \cap \bar{\mathbb{Z}}$.

THEOREM 246. *$\bar{\mathbb{Z}}$ is a ring.* (*Hence $\mathcal{O}_K$ is a ring, the **ring of integers** in K.*)

PROOF. Let $\alpha, \beta \in \bar{\mathbb{Z}}$ satisfy equations

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad \beta^m + b_1\beta^{m-1} + \cdots + b_m = 0$$

with $a_i, b_j \in \mathbb{Z}$. The $\mathbb{Z}$-span of $\{\alpha^i\beta^j\}_{\substack{0 \le i < n \\ 0 \le j < m}}$ is closed under multiplication by α and β, hence by $\alpha + \beta$ and $\alpha\beta$. Set $\gamma := \alpha\beta$ or $\alpha + \beta$, $M_\gamma :=$ the matrix (with entries in $\mathbb{Z}$) of multiplication by γ with respect to the basis $\{\alpha^i\beta^j\}$, and $p_\gamma(\lambda) := \det(\lambda I - M_\gamma)$. Now p_γ is monic and integral, so Cayley-Hamilton $\implies 0 = p_\gamma(M_\gamma) \implies 0 = p_\gamma(\gamma) \implies \gamma \in \bar{\mathbb{Z}}$. □

Now consider two polynomials $f = a_0x^n + \cdots + a_n$ and $g = b_0x^m + \cdots + b_m$ in $\mathbb{Z}[x]$, and assume $\gcd(a_0, \ldots, a_n) = 1 = \gcd(b_0, \ldots, b_m)$. Given any prime p, if a_i and b_j are the coefficients with the smallest subscripts such that $p \nmid a_i$ and $p \nmid b_j$, then it is clear that in $fg =$

$c_0x^{n+m} + \cdots + c_{n+m}$, we have $p \nmid c_{i+j}$. (Why?) Hence $\gcd(c_0, \ldots, c_{n+m}) = 1$.

What if we have two *monic* polynomials $F, G \in \mathbb{Q}[x]$ with $FG = h = x^{m+n} + C_1x^{n+m-1} + \cdots + C_{n+m}$, with all $C_i \in \mathbb{Z}$? Let $\delta_F, \delta_G \in \mathbb{N}$ be the minimal integers required to clear denominators in the coefficients of F resp. G. Then the coefficients of $f := \delta_F F$ have gcd $= 1$, as do those of $g := \delta_G G$, hence those of

$$\delta_G\delta_F h = fg.$$

On the other hand, h is monic, so the gcd of its coefficients is 1, hence the gcd of coefficients of $\delta_G\delta_F h$ is $\delta_G\delta_F$. We conclude that $\delta_G\delta_F = 1$, which is to say F and G were actually integral in the first place.

This demonstrates that if h is reducible in $\mathbb{Q}[x]$, it is actually reducible in $\mathbb{Z}[x]$:

LEMMA 247 (Gauss's Lemma). *If a monic $h \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, it is irreducible in $\mathbb{Q}[x]$.*

Now let $m_\alpha \in \mathbb{Q}[x]$ be the (monic) minimal polynomial of $\alpha \in \bar{\mathbb{Z}}$. By definition, there exists $h \in \mathbb{Z}[x]\backslash\{0\}$ monic with $h(\alpha) = 0$, and we may take h of lowest degree. It is necessarily irreducible in $\mathbb{Z}[x]$: otherwise, $h = h_1h_2$ would imply $h_1(\alpha) = 0$ or $h_2(\alpha) = 0$, contradicting minimality. In $\mathbb{Q}[x]$, we have $m_\alpha \mid h \implies h = m_\alpha g$, which by Gauss ($\implies g \equiv 1$) gives $m_\alpha \in \mathbb{Z}[x]$. That is:

THEOREM 248. *The minimal polynomial of an algebraic integer α belongs to $\mathbb{Z}[x]$, and so its conjugates $\sigma_i(\alpha) \in \bar{\mathbb{Z}}$.*

EXAMPLE 249. $\mathcal{O}_\mathbb{Q} = \mathbb{Q} \cap \bar{\mathbb{Z}} = \mathbb{Z}$. Why? For any $\alpha \in \mathbb{Q}$, the minimal polynomial $m_\alpha = x - \alpha$. If also $\alpha \in \bar{\mathbb{Z}}$, $m_\alpha \in \mathbb{Z}[x]$. So $\alpha \in \mathbb{Z}$.

EXAMPLE 250. Let $K = \mathbb{Q}(\sqrt{d})$, d squarefree. Then I claim that

$$\mathcal{O}_K = \mathbb{Q}(\sqrt{d}) \cap \bar{\mathbb{Z}} = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \underset{(4)}{\equiv} 2,3 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \underset{(4)}{\equiv} 1. \end{cases}$$

For any $\alpha = a + b\sqrt{d} \in K$ (here $a, b \in \mathbb{Q}$), we have

$$m_\alpha(x) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - b^2 d).$$

Now, $\alpha \in \bar{\mathbb{Z}} \iff m_\alpha(x) \in \mathbb{Z}[x] \iff 2a,\ a^2 - b^2 d \in \mathbb{Z} \iff A := 2a,\ B := 2b,\ a^2 - b^2 d \in \mathbb{Z} \iff A,\ B,\ \frac{A^2 - B^2 d}{4} \in \mathbb{Z} \iff A, B \in \mathbb{Z}$ and $A^2 \underset{(4)}{\equiv} B^2 d$. If $d \underset{(4)}{\equiv} 2,3$ (non-QR mod 4) then the only possibility is A, B even. If $d \underset{(4)}{\equiv} 1$ then we musthave A, B even *or* A, B odd.

Now let $K/\mathbb{Q}$ be an algebraic number field of degree n, with embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $i = 1, \ldots, n$, and $\alpha \in K$.

COROLLARY 251. $\alpha \in \mathcal{O}_K \iff m_\alpha \in \mathbb{Z}[x] \iff p_\alpha \in \mathbb{Z}[x]$

$$\iff \begin{cases} Tr_{K/\mathbb{Q}}(\alpha) \\ \quad \vdots \qquad \in \mathbb{Z}, \\ N_{K/\mathbb{Q}}(\alpha) \end{cases}$$

where the "⋮" are the elementary symmetric polynomials[1] *in the conjugates* $\sigma_i(\alpha)$.

(In principle, this gives a method for determining when a given α belongs to $\mathcal{O}_K$.)

PROOF. p_α is a power of m_α, and the numbers $Tr_{K/\mathbb{Q}}(\alpha), \ldots, N_{K/\mathbb{Q}}(\alpha)$ are just the coefficients of $p_\alpha(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$. □

[1]The elementary symmetric polynomials in n variables (or numbers) x_i are $\sum x_i$, $\sum_{i<j} x_i x_j$, $\sum_{i<j<k} x_i x_j x_k$, ..., and $x_1 x_2 \cdots x_n$. The first and last (with $x_i = \sigma_i(\alpha)$) correspond to trace and norm in the Corollary.

DEFINITION 252. The **discriminant** of an n-tuple $\{\alpha_1, \ldots, \alpha_n\} \subset K$ is given by

$$\Delta_{K/\mathbb{Q}}(\underline{\alpha}) := \Delta_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := \det[\underbrace{Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)}_{=:Q(\underline{\alpha})}] \in \mathbb{Q}.$$

(Note that if the $\{\alpha_i\} \subset \mathcal{O}_K$, then this is an integer.)

THEOREM 253. *$\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $K/\mathbb{Q}$ $\iff$ $\Delta_{K/\mathbb{Q}}(\underline{\alpha}) \neq 0$.*

PROOF. ($\Longleftarrow$) If they aren't a basis, there exist $q_i \in \mathbb{Q}$ (not all 0) such that $\sum q_i\alpha_i = 0 \implies \sum q_i\alpha_i\alpha_j = 0\ (\forall j) \implies \sum q_i Tr(\alpha_i\alpha_j) = 0$ $(\forall j)$ which gives a dependency on the rows of $Q(\underline{\alpha}) \implies \det(Q(\underline{\alpha})) = 0$.

($\Longrightarrow$) If they are a basis, but $\Delta(\underline{\alpha}) = 0$, then the system

$$\sum_i x_i Tr(\alpha_i\alpha_j) = 0 \quad (j = 1, \ldots, n)$$

has a nontrivial solution $x_i = q_i \in \mathbb{Q}$, $i = 1, \ldots, n$. Set $\alpha := \sum q_i\alpha_i (\neq 0$, since $\{\underline{\alpha}\}$ is a basis). Then $Tr(\alpha\alpha_j) = 0$ (for $j = 1, \ldots, n$) and (since $\{\underline{\alpha}\}$ is a basis) it follows that $Tr(\alpha\beta) = 0$ $(\forall \beta \in K)$. Taking $\beta = \frac{1}{\alpha}$, we get $0 = Tr(1) = n$, a contradiction. □

Turning to the properties of the discriminant, we have:

PROPOSITION 254. *(i)* $\Delta(\underline{\alpha}) = (\det[\sigma_j(\alpha_i)])^2$
(ii) For $M \in M_n(\mathbb{Q})$ *and*[2] $\underline{\beta} := M\underline{\alpha}$,

$$\Delta(\underline{\beta}) = (\det M)^2\Delta(\underline{\alpha}).$$

PROOF. (i) Consider the matrix equation[3]

$$[Tr(\alpha_i\alpha_j)] = [\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)] = [\sigma_k(\alpha_i)] \cdot {}^t[\sigma_k(\alpha_j)]$$

and take determinant of both sides.

[2] i.e. M is an $n \times n$ matrix and we regard $\underline{\alpha}$, $\underline{\beta}$ as column vectors

[3] here ${}^tM$ is the transpose of M

(ii) The $(i.j)^{\text{th}}$ entry of $M \cdot Q(\underline{\alpha}) \cdot {}^tM$ is:

$$\sum_{k=1}^{n}\sum_{\ell=1}^{n} M_{ik}Tr(\alpha_k\alpha_\ell)M_{j\ell} = Tr\left(\Sigma_k\Sigma_\ell M_{ik}\alpha_k\alpha_\ell M_{jl}\right)$$
$$= Tr\left(\left(\Sigma_k M_{ik}\alpha_k\right)\left(\Sigma_\ell M_{j\ell}\alpha_\ell\right)\right) = Tr(\beta_i\beta_j).$$

So $M \cdot Q(\underline{\alpha}) \cdot {}^tM = Q(\underline{\beta}) \implies$

$$\det(M)\underbrace{\det(Q(\underline{\alpha}))}_{\Delta(\underline{\alpha})}\underbrace{\det({}^tM)}_{\det M} = \underbrace{\det(Q(\underline{\beta}))}_{\Delta(\underline{\beta})}.$$

□

In order to compute some discriminants, we shall need a standard result on Vandermonde determinants:

LEMMA 255. *Let* $\mathbb{F}$ *be a field and* $\{a_i\}_{i=0}^n \subset \mathbb{F}$. *Set*

$$A := \begin{pmatrix} 1 & a_0 & \cdots & a_0^n \\ 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \cdots & a_n^n \end{pmatrix} \in M_{n+1}(\mathbb{F}).$$

Then we have

$$\det(A) = \prod_{n \geq i > j \geq 0} (a_i - a_j).$$

PROOF. Inductive argument with "base case" ($n = 1$)

$$\det\begin{pmatrix} 1 & a_0 \\ 1 & a_1 \end{pmatrix} = a_1 - a_0.$$

Assume the result holds for $n-1$ ($n \times n$ matrices) and prove for n, as follows.

Define a function

$$f(t) := \begin{pmatrix} 1 & a_0 & \cdots & a_0^n \\ 1 & a_1 & \cdots & a_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t & \cdots & t^n \end{pmatrix}$$

and note that $f(a_n) = \det(A)$. By Laplace expansion in the last row, f is a polynomial of degree n, say $\sum_{k=0}^{n} c_k t^k$. In fact, according to that expansion, the coefficient of t^n is

$$c_n = (-1)^{(n+1)+(n+1)} \det \begin{pmatrix} 1 & a_0 & \cdots & a_0^{n-1} \\ 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & \cdots & a_{n-1}^{n-1} \end{pmatrix} = \prod_{n-1 \geq i > j \geq 0} (a_i - a_j),$$

where we have used the inductive hypothesis. Moreover, $f(a_0) = \cdots = f(a_{n-1}) = 0$, since if any of the scalars $a_0, \ldots, a_{n-1}$ are substituted for t, two rows in the matrix are identical (forcing $\det = 0$). Since a polynomial of degree n has at most n roots, this not only tells us all of them – it tells us that f breaks up into linear factors

$$f(t) = c_n(t - a_0) \cdots (t - a_{n-1}) = \prod_{n-1 \geq i > j \geq 0} (a_i - a_j) \times \prod_{n-1 \geq j \geq 0} (t - a_j).$$

So $\det(A) = f(a_n) =$

$$\prod_{n-1 \geq i > j \geq 0} (a_i - a_j) \times \prod_{n-1 \geq j \geq 0} (a_n - a_j) = \prod_{n \geq i > j \geq 0} (a_i - a_j).$$

□

To apply this, write $K = \mathbb{Q}(\theta)$, $p_\theta(X) = \prod_{i=1}^{n}(X - \theta_i) = \prod_{i=1}^{n}(X - \sigma_i(\theta))$, and consider the n-tuple $\Theta := \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$.

THEOREM 256. *$\Delta_{K/\mathbb{Q}}(\Theta) = \prod_{r>s}(\theta_r - \theta_s)^2 = (-1)^{\binom{n}{2}} \prod_{r=1}^{n} p'_\theta(\theta_r) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(p'_\theta(\theta))$. In particular, since the $\{\theta_i\}$ are distinct, $\Delta_{K/\mathbb{Q}}(\Theta) \neq 0$.*

PROOF. Let A denote the matrix

$$\begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix}.$$

Notice that ${}^tA \cdot A = Q(\Theta)$, since their $(i,j)^{\text{th}}$ entries

$$\sum_{k=1}^{n} \theta_k^{i-1}\theta_k^{j-1} = Tr_{K/\mathbb{Q}}(\theta^{i-1}\theta^{j-1})$$

are equal for any (i,j). Since the discriminant is the determinant of $Q(\Theta)$, together with Lemma 255 this gives

$$\Delta(\Theta) = \det({}^tA \cdot A) = (\det A)^2 = \prod_{r>s}(\theta_r - \theta_s)^2.$$

Now $p'_\theta(X) = \sum_{t=1}^{n} \prod_{s\neq t}(X-\theta_s) \implies p'_\theta(\theta_r) = \prod_{s\neq r}(\theta_r - \theta_s)$

$$\implies \prod_{r=1}^{n} p'_\theta(\theta_r) = \prod_{s\neq r}(\theta_r - \theta_s) = (-1)^{\binom{n}{2}} \prod_{r>s}(\theta_r-\theta_s)^2$$

since $\binom{n}{2}$ is the number of factors in the middle product with $r < s$. Noting that $p'_\theta(\theta_r) = p'_\theta(\sigma_r(\theta)) = \sigma_r(p'_\theta(\theta))$, we conclude that

$$\Delta(\Theta) = (-1)^{\binom{n}{2}} \prod_{r=1}^{n} p'_\theta(\theta_r) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(p'_\theta(\theta)).$$

□

A useful computational tool for getting the most out of this is, for $q \in \mathbb{Q}$ and $\alpha \in K$,

$$N(q-\alpha) = \det(\mu_{q-\alpha}) = \det(qI - \mu_\alpha) = p_\alpha(q). \tag{57}$$

EXAMPLE 257. Consider $K = \mathbb{Q}(\theta)$, where $\theta^3 + A\theta + B = 0$ ($A, B \in \mathbb{Q}$). That is, $p_\theta(X) = m_\theta(X) = X^3 + AX + B$, and $[K:\mathbb{Q}] = 3$ (K is a *cubic field*). Noting that $p'_\theta(X) = 3X^2 + A$ and $p'_\theta(\theta) =$

$$3\theta^2 + A = \frac{3\theta^3 + A\theta}{\theta} = \frac{-3A\theta - 3B + A\theta}{\theta} = \frac{-2A\left(-\frac{3B}{2A} - \theta\right)}{0-\theta},$$

we compute (using (57))

$$\Delta_{K/\mathbb{Q}}(\{1,\theta,\theta^2\}) = (-1)^{\binom{3}{2}} N(p'_\theta(\theta)) = -N(3\theta^2 + A)$$

$$= -N(-2A) \times \frac{N\left(-\frac{3B}{2A} - \theta\right)}{N(0-\theta)} = -(-2A)^3 \times \frac{p_\theta\left(-\frac{3B}{2A}\right)}{p_\theta(0)}$$

$$= \frac{8A^3\left(-\frac{27B^3}{8A^3} - \frac{3B}{2} + B\right)}{B} = -\left(27B^2 + 4A^3\right).$$

This should look familiar: $27B^2 + 4A^3$ was the "discriminant of the elliptic curve" given by $Y^2 = X^3 + AX + B$, or more accurately, of the polynomial on its right-hand side.

Exercises

(1) Let $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt[3]{2}$. Compute the norm of $a + b\theta + c\theta^2$ and the discriminant $\Delta(1, \theta, \theta^2)$.
(2) Find $\Delta(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ where $K = \mathbb{Q}(\theta)$, $\theta = \sqrt{2} + \sqrt{3}$.
(3) Compute the minimal polynomial for $\sqrt{3} + \sqrt{7}$.

CHAPTER 32

Ideals in number rings

Let K be an algebraic number field, $\mathcal{O}_K := K \cap \bar{\mathbb{Z}}$ its ring of integers.

LEMMA 258. *Suppose $\beta \in K$. Then there exists $b \in \mathbb{Z}\backslash\{0\}$ such that $b\beta \in \mathcal{O}_K$.*

PROOF. We have $a_0\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0$ ($a_i \in \mathbb{Z}$, $a_0 \neq 0$), and multiplying by a_0^{n-1} gives

$$(a_0\beta)^n + a_1(a_0\beta)^{n-1} + a_2a_0(a_0\beta)^{n-2} + \cdots + a_na_0^{n-1} = 0,$$

so $a_0\beta \in \bar{\mathbb{Z}}$. □

PROPOSITION 259. *Every ideal*[1] *$I \subset \mathcal{O}_K$ contains a basis for $K/\mathbb{Q}$.*

PROOF. Let $\{\beta_1, \ldots, \beta_n\} \subset K$ be a basis. By Lemma 258, there exists a $b \in \mathbb{Z}\backslash\{0\}$ such that $b\beta_1, \ldots, b\beta_n \in \mathcal{O}_K$. Choose $\alpha \in I\backslash\{0\}$; then $b\beta_1\alpha, \ldots, b\beta_n\alpha \in I$, and are a basis for $K/\mathbb{Q}$. □

In fact, every ideal is simply a *lattice* (Prop. below), which is to say that as an additive group it is isomorphic to $\mathbb{Z}^n$. Recall that for $\alpha \in \mathcal{O}_K$, $N(\alpha)$ and $Tr(\alpha)$ belong to $\mathbb{Z}$, and for $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, so does $\Delta(\alpha_1, \ldots, \alpha_n)$.

PROPOSITION 260. *Let $I \subset \mathcal{O}_K$ be an ideal, and $\{\alpha_1, \ldots, \alpha_n\} =: \underline{\alpha} \subset I$ a basis for $K/\mathbb{Q}$ with minimal $|\Delta(\underline{\alpha})| \in \mathbb{N}$. Then*

$$I = \mathbb{Z}\langle\alpha_1, \ldots, \alpha_n\rangle := \{\Sigma_{i=1}^n a_i\alpha_i \mid a_i \in \mathbb{Z}\} \cong \mathbb{Z}^n.$$

(*We say that $\underline{\alpha}$ is an integral basis of I*)

[1] We are tacitly assuming I is not the zero ideal, and shall continue to do so throughout.

PROOF. Given $\alpha \in I$, we have $\alpha = \sum_{i=1}^{n} q_i \alpha_i$, with coefficients $q_i \in \mathbb{Q}$. Suppose some q_i, which we may take to be q_1, is not an integer. Write $q_1 = m + \theta$, where $m \in \mathbb{Z}$ and $\theta \in (0,1)$, and let $\beta_1 = \alpha - m\alpha_1$, $\beta_2 = \alpha_2$, ..., $\beta_n = \alpha_n$. These still belong to I and still give a basis for $K/\mathbb{Q}$. (Why?) Since $\beta_1 = \theta\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n$, the matrix M such that $M\underline{\alpha} = \underline{\beta}$ is

$$M = \begin{pmatrix} \theta & q_2 & q_3 & \cdots & q_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Now $|\Delta(\underline{\beta})| = |(\det M)^2 \Delta(\underline{\alpha})| = \theta^2 |\Delta(\underline{\alpha})| < |\Delta(\underline{\alpha})|$, which contradicts minimality of $|\Delta(\underline{\alpha})|$. Conclude that all $q_i \in \mathbb{Z}$. □

Since any two integral bases for a lattice (such as I) can be expressed in terms of each other (with integer coefficients), the matrix M changing between these bases is invertible over $\mathbb{Z}$. Thus the determinant of M must be ± 1, and so by Prop. 254(ii), the discriminants of the two bases *are the same*.

DEFINITION 261. For an ideal $I \subset \mathcal{O}_K$, define $\Delta(I)$ to be the discriminant of any integral basis of I. The *discriminant of* K is defined by $\delta_K := \Delta(\mathcal{O}_K)$.

EXAMPLE 262. $K = \mathbb{Q}(\sqrt{d})$, d squarefree. First suppose $d \underset{(4)}{\equiv} 2, 3$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ with basis $\alpha_1 = 1$, $\alpha_2 = \sqrt{d}$. Then

$$\delta_K = \det[Tr(\alpha_i \alpha_j)] = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

If $d \underset{(4)}{\equiv} 1$, on the other hand, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ has basis $\alpha_1 = 1$, $\alpha_2 = \frac{1+\sqrt{d}}{2}$, and we have

$$\delta_K = \det[Tr(\alpha_i \alpha_j)] = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

You might think of the discriminant as measuring the "density" of $\mathcal{O}_K$ in K, with a *larger* number indicating that $\mathcal{O}_K$ is more sparse (*less* dense).

LEMMA 263. *Any ideal $I \subset \mathcal{O}_K$ contains a nonzero integer.*

PROOF. Given $\alpha \in I\backslash\{0\}$, $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ for some m and $a_i \in \mathbb{Z}$ (with $a_m \neq 0$). But then $a_m \in I \cap \mathbb{Z}\backslash\{0\}$. □

Recall from §IV.E that we can take the quotient of a ring by an ideal to get a new ring.

PROPOSITION 264. *Let $I \subset \mathcal{O}_K$ be an ideal. Then*[2] *$|\mathcal{O}_K/I| < \infty$.*

PROOF. Let $a \in I \cap \mathbb{Z}\backslash\{0\}$, and let (a) denote the principal ideal generated by a. Since $\mathcal{O}_K/(a) \twoheadrightarrow \mathcal{O}_K/I$ is surjective, it suffices to show that $|\mathcal{O}_K/(a)| < \infty$.

By Prop. 260, we have $\mathcal{O}_K = \mathbb{Z}\langle\omega_1, \ldots, \omega_n\rangle$. Let $\mathcal{S} = \{\sum \gamma_i\omega_i \mid 0 \leq \gamma_i < a,\ \gamma_i \in \mathbb{Z}\}$. Given any $\omega = \sum m_i\omega_i \in \mathcal{O}_K$, write $m_i = q_i a + \gamma_i$ ($\gamma_i, q_i \in \mathbb{Z}$, $0 \leq \gamma_i < a$), so that $\omega \equiv \sum \gamma_i\omega_i \bmod (a)$. Therefore every coset of (a) in $\mathcal{O}_K$ contains an element of $\mathcal{S}$.

If $\sum \gamma_i\omega_i$, $\sum \gamma_i'\omega_i \in \mathcal{S}$ belong to the same coset mod (a), then $\sum(\gamma_i - \gamma_i')\omega_i \in (a) \implies a \mid (\gamma_i - \gamma_i') \implies \gamma_i = \gamma_i'$. So $|\mathcal{O}_K/(a)| = |\mathcal{S}| = a^n < \infty$. □

COROLLARY 265. *Every ascending chain of ideals $I_1 \subset I_2 \subset \cdots$ in $\mathcal{O}_K$ terminates:*[3] *$\mathcal{O}_K$ is a **Noetherian** ring.*

PROOF. Since $\mathcal{O}_K/I_1$ is finite, there are only finitely many ideals containing I_1. □

For the next Corollary, we will need some definitions.

DEFINITION 266. An ideal $P \subset \mathcal{O}_K$ is **prime**
$\iff$ given $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha\beta \in P$, α or β belongs to P
$\iff$ given $\bar{\alpha}, \bar{\beta} \in \mathcal{O}_K/P$ such that $\bar{\alpha}\bar{\beta} \equiv \bar{0}$, $\bar{\alpha}$ or $\bar{\beta} \equiv 0$
$\iff$ $\mathcal{O}_K/P$ is a domain (Defn. IV.E.4).

[2] as usual, $|\cdot|$ denotes the cardinality (number of elements) of a set
[3] i.e. $I_{k+i} = I_k$ $(\forall i \geq 0)$ for some k

DEFINITION 267. An ideal $I \subset \mathcal{O}_K$ is **maximal**
$\iff$ there are no ideals strictly between I and $\mathcal{O}_K$
$\iff$ $\alpha \in \mathcal{O}_K \backslash I \implies I + (\alpha) = \mathcal{O}_K$ ($\implies \exists \beta$: $\alpha\beta \equiv 1 \bmod I$)
$\iff$ $\bar{\alpha} \in \mathcal{O}_K / I \implies \exists \bar{\beta} : \bar{\alpha}\bar{\beta} \equiv \bar{1}$
$\iff$ $\mathcal{O}_K / I$ is a field.

In fact, one can replace $\mathcal{O}_K$ in the above by any commutative ring, and at this level of generality it is always true that maximal ideals are prime (as fields are certainly domains). What is special to the present case (of $\mathcal{O}_K$) is

COROLLARY 268. *Every prime ideal is maximal.*

PROOF. P prime $\implies \mathcal{O}_K / P =: R$ is a domain. So given $a \in R \backslash \{0\}$, the "multiplication by a" map from R to R is 1-to-1 ($ar = ar' \implies a(r - r') = 0 \implies r - r' = 0 \implies r = r'$). But since R is *finite*, 1-to-1 implies bijective; in particular, some element maps to 1, and so a has a multiplicative inverse. Since a was arbitrary, R is a field; hence P is maximal. □

LEMMA 269. *Let $I \subset \mathcal{O}_K$ be an ideal, and $\beta \in K$ be such that $\beta I \subset I$. Then $\beta \in \mathcal{O}_K$.*

PROOF. Exercise. (Use the hypothesis to get a monic integral polynomial relation on β. Similar to an earlier proof.) □

The product IJ of two ideals in a commutative ring R consists of all (finite) sums $\sum a_k b_k$ with $\{a_k\} \subset I$ and $\{b_k\} \subset J$. It is also an ideal.

LEMMA 270. *Given $I, J \subset \mathcal{O}_K$ ideals with $I = IJ$. Then $J = \mathcal{O}_K$.*

PROOF. Write $I = \mathbb{Z}\langle \alpha_1, \ldots, \alpha_n \rangle$. Since $I = IJ$, there exist $\{b_{ij}\} \subset J$ such that (for each i) $\alpha_i = \sum_j b_{ij}\alpha_j$. Writing δ_{ij} for the Kronecker delta (0 if $i \neq j$, 1 if $i = j$), we have (for each i) $0 = \sum_j (b_{ij} - \delta_{ij})\alpha_j$. But this means that the matrix with entries $(b_{ij} - \delta_{ij})$ kills the vector $\underline{\alpha}$, hence has determinant zero. So $0 = \det(B - I)$, and writing out the determinant gives $1 = \sum \prod b'_{ij} s \in J$. Since J contains 1, $J = \mathcal{O}_K$. □

PROPOSITION 271. *Given $I, J \subset \mathcal{O}_K$ ideals, and $\omega \in \mathcal{O}_K$ such that*[4] *$(\omega)I = JI$. Then $(\omega) = J$.*

PROOF. $\beta \in J \implies \beta I \subset JI = (\omega)I = \omega I \implies \frac{\beta}{\omega} I \subset I \implies$ (by Lemma 269) $\frac{\beta}{\omega} \in \mathcal{O}_K \implies \beta \in \omega\mathcal{O}_K = (\omega)$. So $J \subset \omega\mathcal{O}_K = (\omega)$, and $\omega^{-1}J \subset \mathcal{O}_K$ is an ideal satisfying $\omega^{-1}JI = I \implies$ (by Lemma 270) $\omega^{-1}J = \mathcal{O}_K \implies J = (\omega)$. □

Exercises

(1) Prove that a finite commutative domain R is a field. [Hint: given $a \in R$, consider the map from R to itself given by multiplication by a. (Yes, this is in the notes, but try to do it without peeking.)]
(2) Let $I \subset \mathcal{O}_K$ be an ideal, and suppose $\beta \in K$ satisfies $\beta I \subset I$. Show that $\beta \in \mathcal{O}_K$.
(3) Consider the "ideal norm" function $N(I) := |\mathcal{O}_K/I|$. If $I = \mathbb{Z}\langle\beta_1, \ldots, \beta_n\rangle$ and $\mathcal{O}_K = \mathbb{Z}\langle\alpha_1, \ldots, \alpha_n\rangle$, what matrix computes $N(I)$? Using $\beta_i = a\alpha_i$ for $I = (a)$, show that $N((a)) = |N_{K/\mathbb{Q}}(a)|$. [Hint: you should not be taking the determinant of a diagonal matrix of a's here: $a \in \mathcal{O}_K$, not $\mathbb{Z}$.]
(4) Consider the ideals $I = (2, 1 + \sqrt{-29}) = \mathbb{Z}\langle 2, 1 + \sqrt{-29}\rangle$ and $J = (5, 1 - \sqrt{-29}) = \mathbb{Z}\langle 5, 1 - \sqrt{-29}\rangle$ in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-29}]$, where $K = \mathbb{Q}(\sqrt{-29})$. Use problem (3) and Pell's equation, deduce that these ideals are non-principal, i.e. not of the form (a). (Actually, since [as you will see] I and J have prime norm, they have to be prime, but we won't do enough in class to prove that.)

[4]Here $(\omega) = \omega\mathcal{O}_K$ is the principal ideal generated by ω.

CHAPTER 33

The ideal class group

As usual, we let K be an algebraic number field, and $\mathcal{O}_K := K \cap \bar{\mathbb{Z}}$ its ring of integers; denote by $\mathcal{I}(K)$ the *set of nonzero ideals in* $\mathcal{O}_K$. Recall that we can multiply ideals via $IJ := \{\imath\jmath \mid \imath \in I, \jmath \in J\}$, which makes $\mathcal{I}(K)$ into a (commutative) *monoid* (Defn. II.E.1), with identity element given by[1] $\mathcal{O}_K$ itself.

DEFINITION 272. (i) We declare two ideals I, J to be equivalent ($I \sim J$) $\iff$ $\exists\, \alpha, \beta \in \mathcal{O}_K \backslash \{0\}$ such that $(\alpha)I = (\beta)J$.

(ii) Let

$$Cl(K) := \frac{\mathcal{I}(K)}{\sim}$$

denote the set of equivalence classes "$[I]$" (with $[I] = [J] \overset{\text{defn.}}{\iff} I \sim J$). This is called the **ideal class group**.[2]

(iii) Its cardinality $h_K := |Cl(K)|$ is called the **class number** of K.

PROPOSITION 273. $h_K = 1 \iff \mathcal{O}_K$ *is a PID.*[3]

PROOF. ($\implies$) : Let I be an ideal. Since $h_K = 1$, $I \sim \mathcal{O}_K = (1)$, so $\exists \alpha, \beta \in \mathcal{O}_K$ s.t. $(\alpha)I = (\beta)(1) = (\beta)$. Thus $\beta = \alpha\imath$ for some $\imath \in I$, i.e. $\frac{\beta}{\alpha} \in I$, and $I = (\frac{\beta}{\alpha})$. (Why?)

($\impliedby$) : easy! □

In fact, it turns out that

(58)

$\mathcal{O}_K$ PID $\iff$ $\mathcal{O}_K$ UFD (unique factorization domain, cf. §IV.E).

The reason is roughly that the existence of non-principal ideals "aids and abets" non-unique factorization:

[1] That is, $I\mathcal{O}_K = I$ (since $\mathcal{O}_K$ contains 1).

[2] We will have to *prove* that it is a (finite abelian) group, which is done below.

[3] i.e. principal ideal domain: every ideal is of the form (α) for some $\alpha \in \mathcal{O}_K$.

EXAMPLE 274. Let $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and recall the non-unique factorization

$$2 \cdot 3 = 6 = \{1 + \sqrt{-5}\}\{1 - \sqrt{-5}\}$$

of 6 into irreducibles in $\mathcal{O}_K$. On the other hand, the corresponding principal ideals (2), (3), $(1 + \sqrt{-5})$, $(1 - \sqrt{-5})$ decompose further in $\mathcal{I}(K)$:

$$(2) = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}), \quad (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

$$(1 + \sqrt{-5}) = (1 + \sqrt{-5}, 2)(1 + \sqrt{-5}, 3), \quad (1 - \sqrt{-5}) = (1 - \sqrt{-5}, 2)(1 - \sqrt{-5}, 3).$$

Here in each case $(\alpha, \beta) := \{r\alpha + s\beta \mid r, s \in \mathbb{Z}[\sqrt{-5}]\}$ are *non-principal* ideals; that is, they *can't* be written in the form (γ).

REMARK 275. To take the product of two ideals I, J, you take all $\mathcal{O}_K$-lnear combinations of products of elements: e.g., $(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma, \beta\gamma, \alpha\delta, \beta\delta)$.

THEOREM 276. *h_K is always finite.*

We will need a

LEMMA 277. *There is a positive integer M (depending only on K) with the property: given $\alpha, \beta \in \mathcal{O}_K$ ($\beta \neq 0$), there exists $t \in \mathbb{Z}$ ($1 \leq t \leq M$) and an element $\omega \in \mathcal{O}_K$ such that*

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

PROOF. It will suffice to demonstrate the existence of $M \in \mathbb{N}$ such that for each $\gamma \in K$, $|N(t\gamma - \omega)| < 1$ for some $1 \leq t \leq M$ and $\omega \in \mathcal{O}_K$. (Then take $\gamma = \frac{\alpha}{\beta}$.)

So let $\gamma \in K$, and take an integral basis $\{\omega_1, \ldots, \omega_n\} \subset \mathcal{O}_K$. We can write $\gamma = \sum_{i=1}^n \gamma_i \omega_i$, with $\gamma_i \in \mathbb{Q}$. Then

$$|N(\gamma)| = \left| \prod_j \left(\sum_i \gamma_i \sigma_j(\omega_i) \right) \right| \leq \underbrace{\prod_j \left(\sum_i |\sigma_j(\omega_i)| \right)}_{=:C} \cdot \left(\max_i |\gamma_i| \right)^n,$$

and we choose $m \in \mathbb{Z}$, $m > \sqrt[n]{C}$ and set $M := m^n$. (Note that m, C, M don't depend on γ.)

Write $\gamma_i = a_i + b_i$, $a_i \in \mathbb{Z}$ and $b_i \in [0,1)$, $[\gamma] := \sum a_i\omega_i$, $\{\gamma\} := \sum b_i\omega_i$ ($\implies \gamma = [\gamma] + \{\gamma\}$); note that $[\gamma] \in \mathcal{O}_K$. Map $K \xrightarrow{\phi} \mathbb{R}^n$ by

$$\phi(\gamma) := (\gamma_1, \ldots, \gamma_n).$$

For any γ, $\phi(\{\gamma\}) \in [0,1]^n$ = unit cube. Partition this into m^n subcubes of side $\frac{1}{m}$, and consider the points $\phi(\{k\gamma\})$, $1 \le k \le m^n + 1$. By the pigeonhole principle, at least 2 of these points ($\phi(\{h\gamma\})$ and $\phi(\{\ell\gamma\})$, say, with $h > \ell$) lie in the same subcube. Writing $t = h - \ell \le m^n$, we have

$$t\gamma = h\gamma - \ell\gamma = ([h\gamma] - [\ell\gamma]) + (\{h\gamma\} - \{\ell\gamma\}) =: \omega + \delta,$$

where $\omega \in \mathcal{O}_K$ and $\delta = \sum \delta_i\omega_i$ with $|\delta_i| < \frac{1}{m}$. Then $\delta = t\gamma - \omega$ and $|N(\delta)| < C(\frac{1}{m})^n < M(\frac{1}{m})^n = 1$. □

PROOF OF THEOREM 276. Let $I \in \mathcal{I}(K)$. For $\alpha \in I\backslash\{0\}$, $|N(\alpha)| \in \mathbb{N}$. Choose $\beta \in I\backslash\{0\}$ with minimal $|N(\beta)|$. By the Lemma, for any $\alpha \in I$ there is a $t \in \mathbb{Z} \cap [1, M]$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$ with $\omega \in \mathcal{O}_K$. Since $t\alpha - \omega\beta$ belongs to I, by $|N(\beta)|$'s minimality we must have $t\alpha - \omega\beta = 0$. Hence $M!I \subset (\beta) = \beta\mathcal{O}_K$.

Consider the ideal $J = (\frac{1}{\beta})M!I \subset \mathcal{O}_K$, which satisfies $(\beta)J = (M!)I \implies I \sim J$. Since $\beta \in I$, $M!\beta \in (\beta)J$ and so $M! \in J$, which gives $(M!) \subset J$. But then J is sandwiched between $M!\mathcal{O}_K$ and $\mathcal{O}_K$, and is determined by its image $J/M!\mathcal{O}_K$ in $\mathcal{O}_K/M!\mathcal{O}_K$, a finite group. Since the latter has only finitely many subgroups, there are only finitely many possibilities for J, *a fortiori* for $[I]$. Therefore the number of ideal classes is finite. □

PROPOSITION 278. *For any $I \in \mathcal{I}(K)$, there exists $k \in \mathbb{Z} \cap [1, h_K]$ such that I^k is principal.*

PROOF. Since $|Cl(K)| = h_K$, at least two of $I, I^2, \ldots, I^{h_K+1}$ lie in the same class, say $I^i \sim I^j$ with $i < j$. Then there are $\alpha, \beta \in \mathcal{O}_K$ such that $(\alpha)I^i = (\beta)I^j$. Writing $J := I^{j-i}$, we have

$$(\alpha)I^i = (\beta)JI^i \implies (\tfrac{\alpha}{\beta})I^i \subset I^i \implies \omega := \tfrac{\alpha}{\beta} \in \mathcal{O}_K$$

by Lemma 270. Applying Lemma 271, $(\omega)I^i = JI^i \implies J = (\omega)$ is principal. □

Define multiplication in $Cl(K)$ by $[I][J] := [IJ]$; the identity element is the class consisting of all principal ideals, $1 = [(1)] = [\mathcal{O}_K] = [(\alpha)]$ for any $\alpha \in \mathcal{O}_K$. So by the Proposition, $[I^k] = 1 \implies [I^{k-1}][I] = 1$, and $[I]$ has an inverse in $Cl(K)$. This gives

THEOREM 279. *$Cl(K)$ is a finite abelian group, of order h_K.*

Now let $I_1, I_2, J \subset \mathcal{O}_K$ be (nonzero) ideals:

LEMMA 280. (i) $I_1 J = I_2 J \iff I_1 = I_2$.
(ii)[4] $I_2 \supset I_1 \iff \exists I$ *with* $I \cdot I_2 = I_1$ (I_2 *divides* I_1).

PROOF. In each case, ($\Longleftarrow$) is easy, so I'll just prove ($\Longrightarrow$):
(i) Multiply both sides by J^{h_K-1}; since $J^{h_K} = (\alpha)$ (is principal), we have $(\alpha)I_1 = (\alpha)I_2$, hence $I_1 = I_2$.
(ii) Multiply by $I_2^{h_K-1}$ to get $(\beta) \supset I_2^{h_K-1} I_1 \implies I := \frac{1}{\beta} I_2^{h_K-1} I_1 \subset \mathcal{O}_K$ is an ideal. Then $I_2 I = \frac{1}{\beta} I_2^{h_K} I_1 = \frac{1}{\beta}(\beta) I_1 = I_1$. □

THEOREM 281. *Every $I \in \mathcal{I}(K)$ is a product of prime ideals.*

PROOF. Let $I \subsetneq \mathcal{O}_K$ be an ideal. Since $|\mathcal{O}_K / I| < \infty$, I is contained in a *maximal* (proper) ideal P_1. By "Caesar", $I = P_1 J_1$. If $J_1 \neq \mathcal{O}_K$ then $J_1 \subset$ maximal $P_2 \implies I = P_1(P_2 J_2)$. If $J_2 \neq \mathcal{O}_K$ we can continue. By Cor. 265, the ascending chain

$$I \subset J_1 \subset J_2 \subset \cdots$$

must terminate; so we must evidently have $J_t = \mathcal{O}_K$, and then $I = P_1 P_2 \cdots P_t$. □

If P is a prime ideal, then the descending chain $P \supsetneq P^2 \supsetneq P^3 \supsetneq \cdots$ cannot terminate, since then we would have (for some i) $P^i = P^{i+1} \implies P^i = PP^i \implies$ (by Lemma VI.C.13) $\mathcal{O}_K = P$, which is

[4] This is sometimes referred to as **Caesar's Lemma**, since it can be remembered by the line "to divide is to contain".

absurd. Given an ideal $I \subset \mathcal{O}_K$, there is thus a highest power of P containing I:

$$\mathrm{ord}_P I := \text{largest } t \in \mathbb{N} \text{ s.t. } P^t \supset I.$$

LEMMA 282. *Let P be prime, $I, J \in \mathcal{I}(K)$. Then (i) $\mathrm{ord}_P P = 1$, (ii) $\mathrm{ord}_P P' = 0$ for any prime ideal $P' \neq P$, and (iii) $\mathrm{ord}_P IJ = \mathrm{ord}_P I + \mathrm{ord}_P J$.*

PROOF. (i) is clear, and (ii) follows at once from the fact that prime ideals are maximal. For (iii), let $t = \mathrm{ord}_P I$, $s = \mathrm{ord}_P J$. By Caesar, $I = P^t I_1$, $J = P^s J_1$, with $P \not\supseteq I_1, J_1$; hence $IJ = P^{s+t} I_1 J_1$, and (since P is prime[5]) $P \not\supseteq I_1 J_1$. So $s + t = \mathrm{ord}_P IJ$. □

THEOREM 283. *The "prime factorization" of I in Theorem 281 is unique up to reordering of factors.*

PROOF. Write $I = \prod_{P \text{ prime}} P^{a_P}$ by Theorem 281. By Lemma 282, $a_P = \mathrm{ord}_P I$. Therefore the a_P are uniquely determined. □

In view of Theorem 283, we say that $\mathcal{I}(K)$ is a *unique factorization monoid*. This is in contrast to $\mathcal{O}_K$ itself, which (by (58) and Prop. 273) is a unique factorization domain precisely when $Cl(K)$ is trivial (i.e. $h_K = 1$), which is to say not in general. Working with ideals therefore gives us a setting in which unique factorization into primes works unconditionally!

The theory of ideals in rings in fact *began* with ideals in algebraic number rings, invented by Kummer for the express purpose of restoring unique factorization. These "ideal numbers", as he called them, were later abstractified by Dedekind and Emmy Noether for more general rings.

[5]this is a little subtle: since P doesn't contain J_1, there is an element $\jmath_0 \in J_1$ which isn't in P. If $I_1 J_1$ is in P, then all products $\imath \jmath_0$ ($\imath \in I_1$) belong to P. Since P is prime (see the definition in §VI.C), either $\imath$ or $\jmath_0$ is then in P, and as it can't be $\jmath_0$ it must be $\imath$. Since $\imath \in I_1$ was arbitrary, we have $P \supset I_1$, a contradiction.

Exercises

(1) In problem (4) of the last Chapter, determine the orders of I and J in the ideal class group, and deduce that $6|h_K$. (In fact, $h_K = 6$ and $Cl(K) \cong \mathbb{Z}/6\mathbb{Z}$.)

(2) Let I be an ideal of $\mathcal{O}_K$ and suppose that I^r is principal for some $r \in \mathbb{Z}$ with $(h_K, r) = 1$. Show that I is itself principal.

CHAPTER 34

Fermat's Last Theorem for regular exponents

We are now ready to exploit the unique factorization property of $\mathcal{I}(K)$, the monoid of (nonzero) integral ideals in $\mathcal{O}_K$, to study the famous Diophantine equation

$$x^m + y^m = z^m. \tag{59}$$

In order to *disprove* the existence of solutions with nonzero xyz, it is enough to show, for some prime[1] $p \mid m$, that $x^p + y^p = z^p$ has no such solutions.

Cyclotomic fields. This suggests that it will be useful to consider the fields $K = \mathbb{Q}(\zeta_p)$, where p is prime and $\zeta_p = e^{\frac{2\pi i}{p}}$. The key results on these so-called *cyclotomic fields*, for our purposes, are the following:

FACT 284. $K = \mathbb{Q}(\zeta_p) \implies \mathcal{O}_K = \mathbb{Z}[\zeta_p]$, $[K : \mathbb{Q}] = p - 1$.

While we won't prove this, I should mention that the minimal polynomial of ζ_p is not $X^p - 1$ but $\frac{X^p-1}{X-1} = X^{p-1} + \cdots + X + 1$ (which is irreducible over $\mathbb{Q}$); this explains the degree $p - 1$.

FACT 285. *The embeddings $\sigma_j : \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$ $(j = 1, \ldots, p-1)$ are given by sending $\zeta_p \mapsto \zeta_p^j$. Moreover they "respect" complex conjugation: $\sigma_j(\bar{\alpha}) = \overline{\sigma_j(\alpha)}$.*

This one is easy to see: we know there are $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ distinct embeddings; and the $\{\sigma_j\}$ are clearly distinct as ζ_p has distinct images under them. Moreover, an arbitrary element $\alpha = \sum_{k=0}^{p-1} a_k \zeta_p^k$ $(a_k \in \mathbb{Q})$ has image $\sigma_j(\alpha) = \sum a_k \sigma_j(\zeta_p)^k = \sum a_k \zeta_p^{jk}$, and so $\sigma_j(\bar{\alpha}) =$

[1] If $m > 2$ is a power of 2, then $4 \mid m$. We have already checked Fermat for the exponent 4 in §IV.A.

$\sigma_j(\sum a_k\bar{\zeta}_p^k) = \sigma_j(\sum a_k\zeta_p^{-k}) = \sum a_k\zeta_p^{-jk} = \sum a_k\bar{\zeta}_p^{jk} = \overline{\sigma_j(\alpha)}$. Next we have

FACT 286. *The roots of unity in $K = \mathbb{Q}(\zeta_p)$ are just the $\pm\zeta_p^j$.*

If you want to try to prove this, the hint is to first show that in general $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ (clear for $m = p$ from the Fact 284), then ask what happens if $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_p)$.

FACT 287 (Kummer's Lemma). *If $u \in \mathbb{Z}[\zeta_p]^*$, then $u/\bar{u}$ is a root of unity (hence $\pm\zeta_p^j$).*

This is an immediate consequence of the following more general

LEMMA 288 (Kronecker). *Let $K/\mathbb{Q}$ be an algebraic number field, and denote by $\sigma_1, \ldots, \sigma_n$ the n embeddings $K \hookrightarrow \mathbb{C}$. If $\alpha \in \mathcal{O}_K$ is such that $|\sigma_j(\alpha)| \leq 1$ for all $j = 1, 2, \ldots, n$, then α is a root of unity.*

PROOF. Since α is an algebraic integer, it is a root of

$$f(x) = \prod_{j=1}^{n}(x - \sigma_j(\alpha)) = x^n + a_1x^{n-1} + \cdots + a_n$$

where $a_k \in \mathbb{Z}$ for each k. Since $|\sigma_j(\alpha)| \leq 1$ $(\forall j)$, we have also $|a_k| \leq \binom{n}{k}$ for each k. There are only finitely many such polynomials. Moreover, if α satisfies the conditions of the Lemma, then so do its powers $\alpha^2, \alpha^3, \ldots$, which are therefore also among the *finitely many roots* of this set of polynomials. By the pigeonhole principle, two distinct powers of α must be equal. Thus, α is a root of 1. □

Now Fact 287 follows as once, since (using Fact 285) $\sigma_j(u/\bar{u}) = \sigma_j(u)/\sigma_j(\bar{u}) = \sigma_j(u)/\overline{\sigma_j(u)}$ has absolute value 1 for each j.

Fermat's equation. We are interested in the equation

$$x^p + y^p = z^p, \tag{60}$$

where $p > 3$ is prime. The proof that follows really won't work for $p = 3$; fortunately, the exponent 3 can be dealt with by a direct

"argument by descent" as carried out in §IV.A for exponent 4. We won't bother with the details.

Suppose then that there exists a solution, with $xyz \neq 0$. If x, y, z have a common divisor, then of course we can strike it out to get a smaller solution. Assume this done. Now if any two of them still have a common factor m, say $m \mid x, y$, then $m^p \mid z^p \implies (m, z) \neq 1$, a contradiction. So we may assume *x, y, z are pairwise relatively prime*. Also, we *will* assume that *p divides none of them*. A separate, analogous (but more complicated) argument is needed to deal with the case where p divides exactly one of x, y, z. We'll omit this.

So assume $p > 3$ is prime, and (x, y, z) is a solution to (60) in pairwise coprime integers, none divisible by p. We will now attempt to obtain a contradiction by passing to the cyclotomic number ring $\mathbb{Z}[\zeta]$, $\zeta = \zeta_p$, and factoring the left-hand side of (60) to obtain

$$(x + y)(x + y\zeta) \cdots (x + y\zeta^{p-1}) = z^p. \tag{61}$$

Case 1: $\mathbb{Z}[\zeta]$ a UFD. To get started, assume that $h_{\mathbb{Q}(\zeta_p)} = 1$, so that $\mathbb{Z}[\zeta_p]$ is a unique factorization domain: i.e., every element has a factorization into prime elements which is unique up to reordering and units. As

$$(t - \zeta)(t - \zeta^2) \cdots (t - \zeta^{p-1}) = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1}$$

evaluates to p at $t = 1$, we have the inclusion of principal ideals

$$(p) \subset ((1 - \zeta^a))$$

for each $a = 1, 2, \ldots, p - 1$. (Equivalently, $(1 - \zeta^a) \mid p$.) The irreducibility of $1 + t + \cdots + t^{p-1}$ over $\mathbb{Q}$ (implicit in Fact 284) implies that any element of $\mathbb{Q}[\zeta]$ has a unique representation as $a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$.

Next *let $\pi \in \mathbb{Z}[\zeta]$ be a prime factor of $x + y\zeta$*. By unique factorization and (61), $\pi \mid z$. If π also divides $x + y\zeta^{a+1}$ (for some $a = 1, \ldots, p - 1$), then it divides the $\mathbb{Z}[\zeta]$-linear combination $\zeta^{-1}(x + y\zeta) - \zeta^{-1}(x + y\zeta^{a+1}) = y(1 - \zeta^a)$ hence yp. Now in $\mathbb{Z}$, $\gcd(z, yp) \mid \gcd(z, y) \cdot \gcd(z, p) = 1 \cdot 1 = 1 \implies zm + ypm = 1$ for some

$n, m \in \mathbb{Z}$. Since π divides z and yp, we have $\pi \mid 1 \implies \pi \in \mathbb{Z}[\zeta]^*$($\pi$ is a unit) $\implies$ π not prime, a contradiction. So π *divides no other factor in the left-hand side of* (61).

Since π divides z, $\pi^p \mid z^p$. No π-factor can divide other factors (of the left-hand side of (61)), so $\pi^p \mid (x + y\zeta)$. By uniqueness of the decomposition of $x + y\zeta$ into prime factors, and repeating the argument just done for π for the other factors, we find that

$$x + y\zeta = u\alpha^p,$$

for some $\alpha \in \mathbb{Z}[\zeta]$ and $u \in \mathbb{Z}[\zeta]^*$. Write $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$. In $\mathbb{Z}[\zeta]/(p)$, we have[2]

$$\alpha^p \underset{(p)}{\equiv} a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{(p-2)p} \underset{(p)}{\equiv} \sum_{i=0}^{p-2} a_i^p =: a \in \mathbb{Z}/p\mathbb{Z}.$$

By little Fermat, this implies

$$x + y\zeta \underset{(p)}{\equiv} u\alpha^p \underset{(p)}{\equiv} ua \underset{(p)}{\equiv} ua^p$$

hence (applying complex conjugation)

$$x + y\bar{\zeta} \underset{(p)}{\equiv} \bar{u}a^p.$$

Noting that $\bar{\zeta} = \zeta^{-1}$, multiplying by $u/\bar{u}$ gives

$$\frac{u}{\bar{u}}(x + y\zeta^{-1}) \underset{(p)}{\equiv} ua^p \underset{(p)}{\equiv} x + y\zeta^p,$$

which by Kummer's lemma becomes

$$\pm\zeta^k(x + y\zeta^{-1}) \underset{(p)}{\equiv} x + y\zeta$$

so that $p \mid \{x + y\zeta \mp \zeta^k x \mp \zeta^{k-1}y\}$ in $\mathbb{Z}[\zeta]$. By uniqueness of the representation of elements of $\mathbb{Z}[\zeta]$, this is impossible unless $k = 1$.

[2]The first equality here is sometimes called the "freshman's dream" identity. The basic point is that while in the freshman's Calculus class $(x+y)^p = x^p + y^p$ is definitely wrong, in number theory it is true mod p because the $\binom{p}{k}$'s in the binomial expansion are divisible by p. That's the real reason why you aren't allowed to take this course before Calculus.

(Recall $p \nmid x, y$.) Hence $p \mid \{(x \mp y) + \zeta(y \mp x)\} \implies p \mid x \mp y \implies x \underset{(p)}{\equiv} \pm y$.

Writing $x^p + (-z)^p = (-y)^p$, we obtain similarly $x \underset{(p)}{\equiv} \mp z$. If $x \underset{(p)}{\equiv} y$, then $2x^p \underset{(p)}{\equiv} x^p + y^p = z^p \underset{(p)}{\equiv} \mp x^p \implies p \mid 3x^p$ or $p \mid x^p$ (contradiction!). If $x \underset{(p)}{\equiv} -y$, then $0 = x^p - x^p \underset{(p)}{\equiv} x^p + y^p = z^p \implies p \mid z^p$ (contradiction!). (Note that the first contradiction wouldn't go through if $p = 3$.) This completes the argument in Case 1.

Case 2: $\mathbb{Z}[\zeta]$ not a UFD. (i.e., $h_{\mathbb{Q}(\zeta_p)} > 1$) A variant of the above argument was proposed in general by Lamé in 1847. Liouville immediately noticed that if unique factorization didn't hold, the proof was invalid; it turned out that Kummer had already published a proof that it didn't. However, Kummer also pointed out that the proof could be salvaged somewhat by using the unique factorization property for "ideal numbers", as described in the last section.

The question is how far "somewhat" goes. Clearly, we aren't going to prove Fermat's Last Theorem entirely. Wiles's 1995 proof revolves around the modularity of elliptic curves over $\mathbb{Q}$ and requires much more sophisticated methods. So there must be a catch.

But we can still get nonexistence of solutions in some non-UFD cases. Write, in analogy to (61),

$$((x+y))((x+y\zeta))\cdots((x+y\zeta^{p-1})) = (z)^p \tag{62}$$

which is now a factorization into principal ideals. If some prime ideal $\wp$ contains/divides $(x + y\zeta)$, then it can't contain/divide any other on the left-hand side of (62). (Otherwise $\wp \supset (z, yp)$ as before.) Using the unique factorization of ideals in $\mathbb{Z}[\zeta]$ into prime ideals, we get $(x + y\zeta) = I^p$, *I not necessarily principal*.

Now suppose that p is a **regular prime**, i.e.

$$p \nmid h_{\mathbb{Q}(\zeta_p)}.$$

Then $[I] \neq 1 \in Cl(\mathbb{Q}(\zeta_p))$, hence by Lagrange $[I]^p \neq 1 \in Cl(\mathbb{Q}(\zeta_p))$, contradicting principality of $(x + y\zeta)$. (Here, we are using the fact

that an ideal is principal iff its class in $Cl(K)$ is trivial.) Therefore I *must* be principal, i.e. $I = (\alpha)$. Once again, we have $(x + y\zeta) = (\alpha^p)$ $\implies x + y\zeta = u\alpha^p$, and at this point we can just proceed as in Case 1.

Kummer's result. Putting everything together, we arrive at

THEOREM 289 (Kummer, 1847). *There are no solutions with* $x, y, z \in \mathbb{Z}\backslash\{0\}$ *to* (59) *with* m *divisible by* 4 *or a regular prime.*

That is, we have proved Fermat's Last Theorem for (in particular) all exponents up to the first regular prime, which is 37. Note how deeply we dug into the ideal structure of $\mathbb{Z}[\zeta]$ to deal with an equation ostensibly in rational integers!