MATH 2400 ELEMENTARY NUMBER THEORY

DAVID TWEEDLE

These are the course notes for Elementary Number Theory (Math 2400), September 2021. Our source is [Fla18].

Contents

1. Divisibility and primes

Definition 1.1. Let $d \neq 0$ and n be integers. If there exists an integer k such that $n = kd$ then we say that d *divides* n and we write $d|n$. We also say "d is a divisor of n", "d is a factor of n", "n is a multiple of d", "n is divisible by d" to mean that d divides n.

Principle of Mathematical Induction. *Let Q be a subset of $\mathbb{N} = \{1, 2, 3, \ldots, n, \ldots\}$. If*

a) $1 \in Q$ *and*

b) For all $n \geq 1$, if $n \in Q$ then $n + 1 \in Q$

then $Q = \{1, 2, 3, \ldots, n, \ldots\}$.

There is also the well-ordering principle.

Well-ordering Principle. *Suppose that S is a non-empty subset of $\mathbb{N}$. Then S has a least element.*

Date: September 5, 2021.

Proposition 1.2 (Division Algorithm)**.** *Let a and b be integers with $a \neq 0$. Then there exists unique integers q and r such that $0 \leq r < |a|$ and $b = qa + r$.*

Proof. Let a, b be given with $a \neq 0$. Let $S = \{b - qa \mid q \in \mathbb{Z}, b - qa \geq 0\}$. Then S is non-empty (do you see why?). So S has a least element $R \geq 0$. If $R \geq |a|$, then $R - |a| \in S$ as well and $R - |a| < R$ a contradiction. So $0 \leq R < |a|$, as required.

Uniqueness is omitted. □

Definition 1.3. Let $p \geq 2$ be an integer. Then p is called a prime number if its only positive divisors are $1, p$.

Otherwise, p is called a composite number.

The primes are $P = \{2, 3, 5, 7, 11, \ldots\}$ and the composites are $C = \{4, 6, 8, 9, 10, 12, \ldots\}$.

Theorem 1.4. *Every integer $n > 1$ is a product of primes.*

Proof. Let

$$S = \{n \geq 2 | n \text{ cannot be written as a product of primes}\}.$$

Let m be the least element of S. Then $m > 2$ since 2 is prime. So m is composite (otherwise, m is prime itself). Write $m = ab$ where $a, b > 1$. Then $a, b \notin S$, so are products of primes and so is m, a contradiction. □

Definition 1.5. Let a and b be integers, not both zero. An integer c is a common divisor of a and b if $c|a$ and $c|b$. An integer d is a greatest common divisor of a and b if it is a common divisor of a and b and if c is any common divisor of a and b, then $c|d$.

Proposition 1.6. *Let a and b be integers, not both zero. Then* $\gcd(a, b)$ *exists and may be computed in a finite number of applications of the division algorithm*

Proof. Suppose that $b > a > 0$.

$$\begin{aligned}
b &= q_0 a + r_0 \\
a &= q_1 r_0 + r_1 \\
r_0 &= q_2 r_1 + r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

and we claim that $r_n = \gcd(a, b)$. In fact, $\gcd(b, a) = \gcd(q_0 a + r_0, a) = \gcd(r_0, a)$. A similar computation shows $\gcd(r_0, a) = \gcd(r_0, r_1) = \cdots = \gcd(r_n, 0) = r_n$. □

Proposition 1.7. *Suppose that c is a gcd of a and b, where a and b are integers, not both zero. Then there exists integers x and y such that $ax + by = c$.*

Proof. Refer to the computation in Proposition 1.6. We claim that each left hand side may be written as a combination of a and b. Certainly, it is true for both a and b (for example, $b = b \cdot 1 + a \cdot 0$). By induction, assume each of $b, a, r_0, \ldots, r_j$ may be written as $ax + by$. So write $r_j = aX_j + bY_j$ and $r_{j-1} = aX_{j-1} + bY_{j-1}$.

But $r_{j+1} = r_{j-1} - q_{j+1} r_j = a(X_{j-1} - q_{j+1} X_j) + b(Y_{j-1} - q_{j+1} Y_j)$. By induction $r_n = aX + bY$ for some X, Y. □

Lemma 1.8. *Suppose a divides bc and $\gcd(a, c) = 1$. Then a divides b.*

Proof. Write $ax + cy = 1$ by Proposition 1.7. Write $bc = ka$ since a divides bc. Then $b = b \cdot 1 = b(ax + cy) = bax + bcy$. But a divides bax and a divides bcy so a divides their sum, a. □

Theorem 1.9. *Let $n \geq 2$ be an integer. Then n can be written uniquely (up to order) as a product of primes.*

Proof. We have already seen Theorem 1.4 that n can be written as a product of primes. Now, suppose $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ are two representations of a number as a product of primes. Suppose $p_1 \neq q_1$. Then $\gcd(p_1, q_1) = 1$. Then p_1 must divide $q_2 \cdots q_m$ by Lemma 1.8. In this manner, we see that p_1 must be equal to some q_j. So $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_m$ (after relabelling q_j and q_1). By induction, we conclude that these two factorizations are the same after rearrangement, and we are done. □

Proposition 1.10. *Suppose* $\gcd(a, b) = d$. *Then* $\gcd(a/d, b/d) = 1$.

Conversely, if $\gcd(A, B) = 1$ *then* $\gcd(dA, dB) = d$ *for* $d \geq 1$.

Proof. Write $ax + by = d$ by Proposition 1.7. Since $d|a$, $d|b$, a/d and b/d are both integers and

$$(a/d)x + (b/d)y = 1.$$

This implies that $\gcd(a/d, b/d)$ divides 1, and so is equal to 1.

Now, suppose $\gcd(A, B) = 1$. It is clear that $\gcd(Ad, Bd)$ is at least d, as d divides both Ad and Bd. On the other hand, writing $Ax + By = 1$ implies that $Adx + Bdy = d$ and so any divisor of both

Ad and Bd must divide d as well. Therefore, $\gcd(Ad, Bd) = d$, as required. □

Proposition 1.11. *Suppose* $\gcd(a, b, c) = 1$. *Then*

$$\gcd(ab, c) = \gcd(a, c)\gcd(b, c).$$

Proof. Let $e = \gcd(a, c)$ and $f = \gcd(b, c)$. Since $\gcd(a, b, c) = 1$ so too $\gcd(e, f) = 1$. Write $e = ax + cy$ and $f = bu + cv$ for $x, y, u, v \in \mathbb{Z}$ by Proposition 1.7. Then

$$\begin{aligned} ef &= (ax + cy)(bu + cv) \\ &= abxu + bcyu + acxv + c^2vy \\ &= abxu + c(byu + axv + cvy). \end{aligned}$$

This proves that $\gcd(ab, c)$ divides ef. On the other hand, ef divides ab since e divides a and f divides b. We need to show that ef divides c. Write $c = ek$ for some integer k. But f divides c and $\gcd(e, f) = 1$, so f divides k. In other words, $k = f\ell$ wo $c = ef\ell$ and ef divides c. We conclude that $ef \leq \gcd(ab, c)$ so $ef = \gcd(ab, c)$ completing the proof. □

Proposition 1.12. *If* $d|m$ *and* $e|n$ *then* $de|mn$.

Conversely if $\gcd(m, n) = 1$, *then any divisor of* mn *can be written uniquely as* de *where* $d|m$ *and* $e|n$.

Proof. Suppose $D|mn$. Let $d = \gcd(D, m)$ and let $e = \gcd(D, n)$. Then by Proposition 1.11, $de = \gcd(D, mn) = D$.

Suppose $D = d'e'$ where $d'|m$ and $e'|n$ and both d' and e' are positive integers. Then $D = d'e' \leq de = D$, coming from the inequalities $d' \leq d$ and $e' \leq e$. But then $d' = d$ and $e' = e$ as these inequalities must be equalities (else, $D < D$). □

Definition 1.13. Let a, b, c be integers. A linear diophantine equation is an equation of the form

$$aX + bY = c.$$

Remark 1.14. Write $d = \gcd(a, b)$ and suppose $d|c$. Then we may find a solution to $aX + bY = c$ by writing $ax + by = d$ and $c = dk$ and then taking $X = xk$ and $Y = yk$.

Theorem 1.15. *Consider the linear diophantine equation*

$$aX + bY = c. \tag{1}$$

Let $d = \gcd(a, b)$. *Then if* d *does not divide* c, *Equation 1 has no solutions. If* $d|c$, *then let* X_0, Y_0 *be a particular solution to* $aX + bY = c$

(from Remark 1.14). The set of all solutions to Equation 1 is given by

$$\{(X_0 + n(b/d), Y_0 - n(a/d)) \mid n \in \mathbb{Z}\}.$$

Proof. We see that if $d|c$, then a particular solution can be found by solving first $d = ax + by$, and using Proposition 1.7, and then Remark 1.14.

On the other hand, if $aX + bY = c$ for some integers X and Y, certainly $d = \gcd(a, b)$ divides c.

Now, if $aX + bY = c$ and $aX' + bY' = c$, then

$$a(X - X') + b(Y - Y') = 0.$$

So let us examine the equation $ax + by = 0$. The solutions to this equation don't change if we divide through by $d = \gcd(a, b)$. Writing now $(a/d)x = -(b/d)y$, since $\gcd(a/d, b/d) = 1$, y must be a multiple of a/d. So $y = (a/d)n$. Then cancellation gives $x = -(b/d)n$.

So $X = X' - (b/d)n, Y = Y' + (a/d)n$ for some integer n.

That shows that any solution to Equation 1 must be of this form (these are all seen to be solutions of the equation). □

Definition 1.16. Let $S \subseteq \mathbb{Z}$. A common divisor of S is an integer c which divides every element of S. A greatest common divisor of S is a common divisor of S which is divisible by every common divisor of S.

Proposition 1.17. *Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. Let $a = \gcd(a_{n-1}, a_n)$. Then $\gcd(a_1, \ldots, a_n) = \gcd(a_1, \ldots, a_{n-2}, a)$.*

Proof. Omitted. □

2. Modular arithmetic

Let n be a non-zero integer.

Definition 2.1. Let $a, b \in \mathbb{Z}$. Then we say that a is congruent to b modulo n if n divides $b - a$. In that case, we write $a \equiv b \bmod n$.

Proposition 2.2.

- *If $a \equiv b \bmod n$ then $b \equiv a \bmod n$.*
- *For all a, $a \equiv a \bmod n$.*
- *If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$.*

Proof. Omitted. □

Definition 2.3. Let $m \neq 0$. The integers modulo m are defined to be the set of congruence classes modulo m. If $a \in \mathbb{Z}$, the congruence class of a modulo m is denoted $\overline{a}$ and

$$\overline{a} = \{x \in \mathbb{Z} \mid m|x-a\} = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}.$$

The set of integers modulo m is denoted $\mathbb{Z}/m\mathbb{Z}$. If $a, b \in \mathbb{Z}$, we define $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$.

Proposition 2.4. *Suppose $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$. Then $ab \equiv a'b' \bmod m$ and $a + b \equiv a' + b' \bmod m$.*

Proof. Omitted. □

Remark 2.5. Note that $\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ and there are m congruence classes modulo m.

Definition 2.6. Let $m \neq 0$ be an integer. Let $a \in \mathbb{Z}$. Then a is called invertible modulo m if there exists $b \in \mathbb{Z}$ such that

$$ab \equiv 1 \bmod m.$$

Similarly, if $\alpha \in \mathbb{Z}/m\mathbb{Z}$, then α is called invertible if there exists $\beta \in \mathbb{Z}/m\mathbb{Z}$ such that $\alpha\beta = 1$.

The set of all invertible congruence classes modulo m is denoted U_m.

Proposition 2.7. *Let $\alpha = \overline{a} \in \mathbb{Z}/m\mathbb{Z}$. Then $\alpha \in U_m$ if and only if $\gcd(a, m) = 1$.*

Proof. Suppose $ab \equiv 1 \bmod m$. Then there exists d such that

$$ab + md = 1.$$

This implies that $\gcd(a, m) = 1$.

Now, suppose $\gcd(a, m) = 1$ and write $ab + md = 1$. This implies $ab \equiv 1 \bmod m$ and so a is invertible modulo m. □

Remark 2.8. Let p be prime. Then U_p has $p - 1$ elements.

Theorem 2.9. *Let $a \in \mathbb{Z}$. Then*

$$a^p \equiv a \bmod p.$$

Proof. Recall Lagrange's Theorem from Group Theory. This tells us that $\overline{a}^{p-1} = \overline{1}$ for all $\overline{a} \in U_p$.

Alternatively, consider

$$\begin{array}{cccccc} 1, & 2, & 3, & \ldots, & p-1 \\ a, & 2a, & 3a, & \ldots, & a(p-1) \end{array}.$$

Both sequences give a complete set of representatives modulo p.

We then have

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv a \cdot 2a \cdot 3a \cdots a(p-1) \bmod m$$

Cancelling $1, 2, 3, \ldots, p-1$ on both sides gives

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

□

Theorem 2.10. *Let p be prime. Then $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Proof. Omitted. □

Theorem 2.11. *Let $\varphi(m) = |U_m|$ for $m \geq 2$. Then if $\overline{a} \in U_m$, we have $\overline{a}^{\varphi(m)} = \overline{1}$.*

Proof. Omitted. □

Proposition 2.12. *Let $d = \gcd(a, m)$. The congruence equation*

$$ax \equiv b \bmod m$$

has a solution $x \in \mathbb{Z}$ if and only if d divides b.

Proof. Rewrite $ax \equiv b \bmod m$ as

$$ax + my = b,$$

and apply Proposition 1.7. □

Proposition 2.13. *Suppose d divides N. Then define $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ by the rule*

$$f(\overline{a}) = \overline{a}.$$

(This function takes an integer modulo m and reduces it modulo d). Then f is a well-defined homomorphism.

Proof. Suppose $a \equiv b \bmod m$. We must show that $f(\overline{a}) = f(\overline{b})$. So m divides $b - a$ by the definition of divides (Definition 1.1). But d divides m and so also divides $b - a$. So $a \equiv b \bmod d$ as required.

It is clear that f is a homomorphism as long as f is well-defined. □

Theorem 2.14. *Define $F : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by the rule $F(\overline{a}) = (\overline{a}, \overline{a})$ where the first coordinate is $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ and the second coordinate is $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. is a modulo n.*

Then F is an isomorphism of rings.

Proof. First, we show that F is well-defined. Then we show that F is a homomorphism. Then we show that F is 1–1 and onto.

Our definition of F is well-defined as long as each component function is well-defined. So we need to know that for a divisor d of N, the function

$$\overline{a} \in \mathbb{Z}/N\mathbb{Z} \mapsto \overline{a} \in \mathbb{Z}/d\mathbb{Z}$$

is well-defined. This is Proposition 2.13.

Since each coordinate of F is a homomorphism, so too is F.

The tricky part is to prove that F is 1–1 and onto.

Let $(\overline{a}, \overline{b}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Write $mx + ny = 1$ since $\gcd(n, m) = 1$ and using Proposition 1.7. Let $A = nya + mxb$. Then $A \equiv nya \equiv a \bmod m$ and $A \equiv mxb \equiv b \bmod n$. So $F(\overline{A}) = (\overline{a}, \overline{b})$. So F is onto. The function F must therefore be 1–1 as well since $\mathbb{Z}/mn\mathbb{Z}$ has the same number of elements as $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

3. Arithmetic functions

This week, we will discuss arithmetic functions. That is functions $f : \mathbb{N} \to \mathbb{C}$ which carry some arithmetic meaning.

Definition 3.1. For $n \in \mathbb{N}$, define $d(n) = \sum_{d|n} 1$, the sum being over positive divisors of n. In other words, $d(n)$ gives the number of divisors of n. We can examine the average value of $d(n)$. First, we need three definitions.

Definition 3.2. Let $x \in \mathbb{R}$. Define the greatest integer part of x, denoted $\lfloor x \rfloor$, by

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z} \text{ such that } n \leq x\}.$$

Definition 3.3. We write $f(x) = \mathrm{O}(g(x))$, if there exists a positive real constant $C > 0$ and a real number x_0 such that

$$|f(x)| \leq Cg(x)$$

for all $x \geq x_0$.

Definition 3.4. The Euler-Mascheroni constant, denoted γ, is defined by

$$\gamma = \lim_{n\to\infty} \left[\left(\sum_{k=1}^{n} \frac{1}{k} \right) - \log n \right].$$

Proposition 3.5. *We have the estimate*

$$\sum_{n \leq X} 1/n - \log X = \gamma + \mathrm{O}(1/X),$$

as $X \to \infty$, where γ is the Euler-Mascheroni constant.

Proof. This proof uses the Euler summation formula, if you are interested. First, write

$$\log X = \int_1^X 1/t \, dt.$$

Then write

$$1/t = (t - \lfloor t \rfloor)/t^2 + \lfloor t \rfloor / t^2,$$

and substitute into the integral. First, note that

$$\int_1^X (t - \lfloor t \rfloor)/t^2 \, dt = \mathrm{O}(1/X).$$

Now, notice that

$$\begin{aligned}
\int_1^X \lfloor t \rfloor / t^2 \, dt &= \sum_{1 \le n \le X} \int_{n-1}^{n} (n-1)/t^2 \, dt + \int_{\lfloor X \rfloor}^{X} \lfloor X \rfloor / t^2 \, dt \\
&= \sum_{1 \le n \le X} (n-1) \left(1/(n-1) - 1/n\right) \\
&\quad + \lfloor X \rfloor (1/\lfloor X \rfloor - 1/X) \\
&= \sum_{1 \le n \le X} (1 - (n-1)/n) + \frac{X - \lfloor X \rfloor}{X} \\
&= \sum_{1 \le n \le X} 1/n + \mathrm{O}(1/X).
\end{aligned}$$

So we conclude that

$$\log X = \sum_{1 \le n \le X} 1/n + \mathrm{O}(1/X)$$

as $X \to \infty$. □

Proposition 3.6. *The mean value of $d(n)$ for $n \le X$ is approximately $\log X + 2\gamma - 1$. Here, γ is the Euler-Mascheroni constant defined by*

$$\gamma = \lim_{n \to \infty} \left(\sum_{k=1}^{n} 1/k - \log n \right).$$

Proof. Let

$$S(X) = \sum_{n \le X} d(n),$$

where the sum is over positive integers n. Our goal is to prove that

$$S(X) = X \log X + X(2\gamma - 1) + \mathrm{O}(\sqrt{X}).$$

First, write

$$S(X) = \sum_{n \le X} \sum_{n=dk} 1.$$

Then write

$$S(X) = \sum_{d,k,dk \le X} 1$$

Consider a term in $S(X)$ corresponding to d, k with $dk \le X$. Then either $d \le k$ or $k < d$. Let us consider the sum of terms with $d \le k$. Since $d \le k$ and $dk \le X$, we have $d \le \sqrt{X}$. For d fixed, the total contribution is $\lfloor X/d \rfloor - d + 1$. (The admissable k for this d are $k = d, d+1, d+2, \ldots, \lfloor X/d \rfloor$). So the total for $d \le k$ is

$$\sum_{d \le \sqrt{X}} (\lfloor X/d \rfloor - d + 1).$$

Similarly, the total for $k < d$ is

$$\sum_{k \le \sqrt{X}} (\lfloor X/k \rfloor - d).$$

In total,

$$S(X) = 2 \sum_{d \le \sqrt{X}} (\lfloor X/d \rfloor) - 2 \sum_{d \le \sqrt{X}} d + \mathrm{O}(\sqrt{X}).$$

Now, we must estimate $\sum_{d \le \sqrt{X}} 1/d$ and $\sum_{d \le \sqrt{X}} d$. Write

$$\sum_{d \le \sqrt{X}} 1/d = \log(\sqrt{X}) + \gamma + \mathrm{O}(1/\sqrt{X})$$

by Proposition 3.5. Then write

$$\sum_{d \le \sqrt{X}} d = \lfloor \sqrt{X} \rfloor \cdot (\lfloor \sqrt{X} \rfloor - 1)/2$$

In total,

$$\begin{aligned} S(X) &= 2X(\log(\sqrt{X}) + \gamma + \mathrm{O}(1/\sqrt{X})) + X + \mathrm{O}(\sqrt{X}) \\ &= X \log X + (2\gamma - 1)X + \mathrm{O}(\sqrt{X}). \end{aligned}$$

□

Definition 3.7. In a similar vein, define $\sigma(n) = \sum_{d|n} d$, and in general, $\sigma_k(n) = \sum_{d|n} d^k$.

Definition 3.8. Define $\phi(n) = |U_n|$ for $n \geq 1$. By Proposition 2.7,

$$\phi(n) = \sum_{1 \leq d \leq n,\ \gcd(d,n)=1} 1$$

and so

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \sum_{k \leq d, \gcd(k,d)=1} 1 = n. \tag{2}$$

Proposition 3.9. *There exists a function $\mu : \mathbb{N} \to \{\pm 1\}$ such that for all functions $f, g : \mathbb{N} \to \mathbb{C}$, the following are equivalent*

a) for all $n \in \mathbb{N}$, $f(n) = \sum_{d|n} g(d)$,
b) for all $n \in \mathbb{N}$, $g(n) = \sum_{d|n} \mu(d) f(d/n)$.

Proof. First, define a function f by the rule $f(n) = 1$ for all $n \in \mathbb{N}$ and define g by the rule

$$g(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

So, we have

$$f(n) = \sum_{d|n} g(d),$$

for all $n \in \mathbb{N}$. We want to find a function μ such that

$$g(n) = \sum_{d|n} \mu(d) f(n/d). \tag{3}$$

Certainly, we may take $\mu(1) = 1$ so that Equation 3 holds when $n = 1$.

Now, assume $\mu(k)$ has been defined for all $1 \leq k \leq n$, and Equation 3 holds for all $1 \leq k \leq n$. Consider

$$g(k+1) = \sum_{d|k+1, d<k+1} \mu(d) f(n/d) + \mu(k+1) f(1),$$

and notice that all terms have been determined except $\mu(k+1)$. In particular,

$$\mu(k+1) = - \sum_{d|k+1, d<k+1} \mu(d).$$

This proves the existence of $\mu(n)$, and we see that μ is also unique (although we didn't mention this).

Now, suppose $F(n) = \sum_{d|n} G(n)$ for all $n \in \mathbb{N}$. Then

$$\begin{aligned}\sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n} \mu(d) \sum_{e|(n/d)} G(e) \\ &= \sum_{e|n} G(e) \sum_{d|(n/e)} \mu(d) \\ &= \sum_{e|n} G(e) \begin{cases} 1 & \text{if } n/e = 1 \\ 0 & \text{if } n/e > 1 \end{cases} \\ &= G(n).\end{aligned}$$

Now, assume $G(n) = \sum_{d|n} \mu(d)F(n/d)$. Then

$$\begin{aligned}\sum_{d|n} G(n) &= \sum_{d|n} \mu(d) \sum_{e|(n/d)} F(e) \\ &= \sum_{e|n} F(e) \sum_{d|(n/e)} \mu(d) \\ &= \sum_{e|n} F(e) \cdot \begin{cases} 1 & \text{if } n/e = 1 \\ 0 & \text{if } n/e > 1 \end{cases} \\ &= F(n)\end{aligned}$$

□

Definition 3.10. The function μ constructed in Proposition 3.9 is called the Möbius function.

Definition 3.11. Let $g : \mathbb{N} \to \mathbb{C}$ be a function. Then g is called multiplicative if $g(mn) = g(m)g(n)$ for all m, n such that $\gcd(m, n) = 1$.

The function g is called completely multiplicative if $g(mn) = g(m)g(n)$ for all $m, n \in \mathbb{N}$.

Proposition 3.12. *The Möbius function μ is multiplicative. That is, for all m, n with $\gcd(m, n) = 1$, we have*

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

Proof. We prove that for all N, if $N = mn$ with $\gcd(m, n) = 1$ then $\mu(mn) = \mu(m)\mu(n)$. We proceed by induction on N, the base case being trivial.

Let N now be given and write $N = mn$ with $\gcd(m, n) = 1$.

By definition of μ, we have

$$\begin{aligned}\mu(n) + \sum_{d|n,d<n} \mu(d) &= 0\\ \mu(m) + \sum_{d|m,d<m} \mu(d) &= 0\\ \mu(mn) + \sum_{d|mn,d<mn} \mu(d) &= 0\end{aligned}$$

Now, multiply the first two above equations to get

$$\begin{aligned}\mu(n)\mu(m) + \sum_{d|n,d<n} \mu(m)\mu(d)& \\ + \sum_{d|m,d<m} \mu(d)\mu(n) + \sum_{d_1|m,d_2|n} \mu(d_1)\mu(d_2) &= 0.\end{aligned}$$

Except for the first term, the induction hypothesis allows us to write

$$\mu(n)\mu(m) + \sum_{d|n,d<n} \mu(md) + \sum_{d|m,d<m} \mu(dn) + \sum_{d_1|m,d_2|n} \mu(d_1d_2) = 0.$$

But the last three sums cover all possibilities of divisors $d|mn$ with $d < mn$ by Proposition 1.12. Now since $\mu(mn) + \sum_{d|mn,d<mn} \mu(d) = 0$, we obtain that $\mu(mn) = \mu(m)\mu(n)$.

By induction, we are done. □

Proposition 3.13. *Suppose that f, g are arithmetic functions such that*

$$f(n) = \sum_{d|n} g(n),$$

for all $n \in \mathbb{N}$.

Then f is multiplicative if and only if g is multiplicative.

Proof. Suppose g is multiplicative and $f(n) = \sum_{d|n} g(d)$. Suppose $\gcd(m, n) = 1$. Then

$$f(mn) = \sum_{d|mn} g(d).$$

For each $d|mn$ we can write $d = d_1d_2$ where $d_1 = \gcd(m, d)$, $d_2 = \gcd(n, d)$ by Proposition 1.12, and $\gcd(d_1, d_2) = 1$.

Furthermore, $g(d_1d_2) = g(d_1)g(d_2)$ since $\gcd(d_1, d_2) = 1$. Now,

$$\begin{aligned} f(m)f(n) &= \sum_{d_1|m} g(d_1) \sum_{d_2|n} g(d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} g(d_1)g(d_2) \\ &= \sum_{d_1d_2|mn} g(d_1d_2) \\ &= \sum_{d|mn} g(d) \\ &= f(mn) \end{aligned}$$

which proves that f is multiplicative if g is.

Suppose now that f is multiplicative and $g(n) = \sum_{d|n} \mu(d)f(n/d)$.

$$\begin{aligned} g(m)g(n) &= \sum_{d_1|m} \mu(d_1)f(m/d_1) \sum_{d_2|n} \mu(d_2)f(n/d_2) \\ &= \sum_{d|mn} \mu(d)f(mn/d) \end{aligned}$$

the proof being much the same as for the previous case, except that we also need that $\mu(\cdot)$ is multiplicative as well. Using Proposition 3.12 completes the proof. □

4. Polynomials

Definition 4.1. Let n be a non-zero integer. A polynomial with coefficients in $(\mathbb{Z}/n\mathbb{Z})[x]$ is defined to be

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k,$$

where $a_0, a_1, \ldots, a_k \in (\mathbb{Z}/n\mathbb{Z})$.

If $a_k \neq 0$, the degree of f is said to be k, and we write $\deg f = k$.

The set of all polynomials with coefficients in $(\mathbb{Z}/n\mathbb{Z})[x]$ is denoted $(\mathbb{Z}/n\mathbb{Z})[x]$.

Remark 4.2. Let p be a prime number. The polynomials modulo p, $(\mathbb{Z}/p\mathbb{Z})[x]$, behave nicely.

If $f, g \in (\mathbb{Z}/p\mathbb{Z})[x]$ and $f, g \neq 0$, then $\deg fg = \deg f + \deg g$.

This is not true modulo for polynomials in $(\mathbb{Z}/6\mathbb{Z})[x]$.

From now on, we will look at polynomials modulo p, where p is prime.

Definition 4.3. Let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ be a polynomial. We say that $\alpha \in (\mathbb{Z}/p\mathbb{Z})$ is a root of $f(x)$ if $f(\alpha) = 0$.

Proposition 4.4. *Let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ and let $\alpha \in (\mathbb{Z}/p\mathbb{Z})$. Then $f(\alpha) = 0$ if and only if there exists $g(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ such that $f(x) = (x - \alpha)g(x)$.*

Proof. Omitted. □

Proposition 4.5. *Let $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ of degree n. Then $f(x)$ has at most n roots in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. We proceed by induction on $n = \deg f$. The degree 0 polynomials are the non-constant polynomials $f(x) = c \in \mathbb{Z}/p\mathbb{Z}$. The proposition holds for these.

Now, assume that the proposition holds for all f of degree $n - 1$. Let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be degree n. If f has no roots, we are done. Otherwise, let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ be such that $f(\alpha) = 0$. By Proposition 4.4, there exists $g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ such that $f(x) = (x - \alpha)g(x)$. We have that $\deg f = \deg g + \deg(x - \alpha)$ so that $\deg g = n - 1$. So g has at most $n - 1$ roots in $\mathbb{Z}/p\mathbb{Z}$ and f has at most n roots in $\mathbb{Z}/p\mathbb{Z}$, and we are done by induction. □

5. Primitive roots

Definition 5.1. Let $n \geq 2$ be an integer. Let $\overline{a} \in U_n$. Then the order of a modulo n is defined to be the least positive integer d such that $\overline{a}^d = \overline{1}$.

Proposition 5.2. *Let $\overline{a} \in U_n$. Let d be the order of $\overline{a}$. Then*

$$1, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{d-1}$$

are distinct. Furthermore, if $\overline{a}^i = \overline{a}^j$ for two integers i, j then $i \equiv j \bmod d$.

Proof. First, suppose that $\overline{a}^j = \overline{1}$ for some integer $j \geq 1$. Then use the division algorithm to write $j = qd + r$ where $0 \leq r \leq d - 1$ and $q \in \mathbb{Z}$. Then

$$\begin{aligned}
\overline{1} &= \overline{a}^j \\
&= \overline{a}^{qd+r} \\
&= (\overline{a}^d)^q \cdot \overline{a}^r \\
&= \overline{1}^q \overline{a}^r \\
&= \overline{a}^r
\end{aligned}$$

Now, $\overline{a}^r = \overline{1}$ and $0 \leq r \leq d - 1$ so since d is the minimal positive integer such that $\overline{a}^d = \overline{1}$, we must have $r = 0$. That is, d divides j.

Now, suppose $\overline{a}^i = \overline{a}^j$. Then $\overline{a}^{i-j} = \overline{1}$ and $i \equiv j \bmod d$ from the previous argument.

Finally, this tells us that $\overline{1}, \overline{a}, \ldots, \overline{a}^{d-1}$ are all distinct since the difference of any two exponents will not be divisible by d. $\square$

Definition 5.3. Let $a \in \mathbb{Z}$ and let $n \geq 2$ be an integer. Then a is called a primitive root modulo n if the order of a modulo n is equal to $|U_n| = \varphi(n)$.

Proposition 5.4. *Let $n \geq 2$ be an integer. The following are equivalent:*

a) a is a primitive root modulo n
b) for every prime q dividing $\varphi(n)$, we have $\overline{a^{\varphi(n)/q}} \neq \overline{1}$
c) we have $U_n = \{\overline{a}^n \mid n \in \mathbb{Z}\}$

Proof. Assume a is a primitive root modulo n. That is, assume the order of a modulo n is equal to $\varphi(n)$ which is equal to the number of elements of U_n, by Proposition 2.7, and the definition of $\varphi(n)$ (Definition 3.8). Then, if $d = \varphi(n)$, then $1, \overline{a}, \overline{a}^2, \ldots, \overline{a}^{d-1}$ are all distinct (Proposition 5.2). So, $\{\overline{1}, \overline{a}, \ldots, \overline{a}^{d-1}\} \subseteq U_n$ and both sets have $\varphi(n) = d$ elements, so $U_n = \{\overline{1}, \overline{a}, \ldots, \overline{a}^{d-1}\}$.

Assume $U_n = \{\overline{a}^n \mid n \in \mathbb{Z}\}$. Let d be the order of a modulo n. Then $\{\overline{a}^n \mid n \in \mathbb{Z}\}$ has d elements by Proposition 5.2 and since $d = \varphi(n)$, we have that a is a primitive root modulo n.

Assume that a is a primitive root modulo n. Suppose $\overline{a}^{\varphi(n)/q} = \overline{1}$ for some prime q dividing $\varphi(n)$. Then the order of a modulo n is at most $\varphi(n)/q < \varphi(n)$ so that a is not a primitive root modulo n, a contradiction. Therefore, $\overline{a}^{\varphi(n)/q} \neq \overline{1}$ for every prime q dividing $\varphi(n)$.

On the other hand, suppose that a is not a primitive root modulo n. Let the order of a modulo n be $d < \varphi(n)$ and let $m = \varphi(n)/d$ and let q be a prime divisor of m. Then

$$\begin{aligned}\overline{a}^{\varphi(n)/q} &= \overline{a}^{\varphi(n)/d \cdot d/q} \\ &= (\overline{a}^m)^{d/q} \\ &= \overline{1}\end{aligned}$$

as required.

We have now shown the equivalence of all three conditions in the statement of the proposition. $\square$

Theorem 5.5. *Let p be a prime. Then there exist primitive roots modulo p. In other words, there is $\alpha \in U_p$ such that $U_p = \{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$.*

Proof. Let $A(d)$ be the number of elements of U_p of order d, where d divides $p - 1$.

Each element of order *dividing* d is a root of the polynomial $x^d - 1$. Furthermore, there are exactly d elements of U_p of order dividing d.

To see why, notice that $x^{p-1}-1$ has exactly $p-1$ roots modulo p Theorem 2.9 and Proposition 4.5.

Now, let d divide $p-1$ and see that $x^{p-1}-1 = (x^d-1)(1+x^d+x^{2d}+\cdots+x^{d\cdot[(p-1)/d-1]})$. Since $x^{p-1}-1$ has exactly $p-1$ distinct roots, so too does x^d-1 have exactly d distinct roots.

This proves that $d = \sum_{k|d} A(k)$ for each d dividing $p-1$. By Möbius inversion Proposition 3.9,

$$A(k) = \sum_{d|k} \mu(k/d)\cdot d = \phi(k).$$

In particular, $A(p-1) = \phi(p-1) > 0$ so that there exist primitive roots modulo p. □

Proposition 5.6. *Let p be a prime number. Then a is a primitive root modulo p if and only if for all primes q dividing $p-1$, there is no solution to the equation $\overline{b}^q = \overline{a}$.*

Proof. Suppose that q divides $p-1$ and there exists $b \in \mathbb{Z}$ such that $\overline{b}^q = \overline{a}$. Then $\overline{a}^{(p-1)/q} = (\overline{b}^q)^{(p-1)/q} = \overline{b}^{q-1} = \overline{1}$. By Proposition 5.4, a is not a primitive root modulo p.

Suppose that a is not a primitive root modulo p. Then $\overline{a}^{(p-1)/q} = \overline{1}$ for some prime q dividing $p-1$ by Proposition 5.4. Let $\overline{b}$ be a primitive root modulo p (by applying Theorem 5.5). Write $\overline{b}^j = \overline{a}$. If $j = qm$ then we are done since $\overline{a} = \overline{b}^j = (\overline{b}^m)^q$. Now, divide j by q to get $j = mq + r$ where $0 \le r < q-1$. Now see that $\overline{a}^{(p-1)/q} = \overline{b}^{(p-1)/q\cdot r} \neq \overline{1}$ since $\overline{b}$ is a primitive root. This is a contradiction so j divides q, so there exists a solution to $\overline{\beta}^q = \overline{a}$ for some prime q dividing $p-1$. □

Theorem 5.7. *Let $p > 2$ be a prime number and $r \ge 1$ be an integer. If $n = 2, 4$, $n = p^r$ or $n = 2p^r$ then there are primitive roots modulo n.*

In any other case, (if 4 divides $n > 4$ or if n has two distinct odd prime divisors), then there are no primitive roots modulo n.

Proof. Omitted. □

6. Quadratic residues

Definition 6.1. Let p be a prime and let $\overline{a} \in U_p$. We say that a is a quadratic residue modulo p if there exists $\overline{b} \in U_p$ with $\overline{a} = \overline{b}^2$.

We define the Legendre symbol $\left(\frac{a}{p}\right)$ for $p \nmid a$ by the rule

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \end{cases}$$

Proposition 6.2. *Let p be an odd prime. Then there are $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ quadratic non-residues modulo p.*

Proof. The quadratic residues modulo p are

$$\overline{1}^2, \overline{2}^2, \ldots, \overline{(p-1)/2}^2, \overline{(p+1)/2}^2, \ldots, \overline{p-1}^2.$$

But $\overline{1}^2 = \overline{p-1}^2$, $\overline{2}^2 = \overline{p-2}^2$, and so on. So the complete list of quadratic residues modulo p are

$$\overline{1}^2, \ldots, \overline{(p-1)/2}^2.$$

We claim that these are all distinct modulo p. If $1 \leq i \leq j \leq (p-1)/2$ and $\overline{i}^2 = \overline{j}^2$ then

$$0 \equiv i^2 - j^2 \equiv (i-j)(i+j) \bmod p,$$

which implies that p divides $j-i$ or $i+j$. But $1 \leq i+j \leq p-1$ so it is impossible for $i+j$ to be divisible by p. So p divides $j-i$. But $0 \leq j-i \leq (p-1)/2$ so in order to be divisible by p, it must be that $j-i=0$.

This proves that $\overline{1}^2, \overline{2}^2, \ldots, \overline{(p-1)/2}^2$ are all distinct, so there are exactly $(p-1)/2$ quadratic residues modulo p. □

Proposition 6.3. *Let p be an odd prime. Suppose $\gcd(p,a)=1$. Then*

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

Proof. Let $f(x) = x^{p-1} - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$. Notice that

$$f(x) = (x^{p-1}-1) = (x^{(p-1)/2}-1)(x^{(p-1)/2}+1)$$

as polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$. By Theorem 2.9, every element of U_p is a root of $f(x)$. There are $p-1$ elements of U_p, so by Proposition 4.5, the roots of $f(x)$ are exactly the elements of U_p. Therefore, each element of U_p either satisfies $a^{(p-1)/2} = 1$ or $a^{(p-1)/2} = -1$.

We now claim that the quadratic residues modulo p are the roots of $x^{(p-1)/2} - 1$ and the nonresidues are the roots of $x^{(p-1)/2} + 1$. First, suppose $\overline{b}^2 = \overline{a}$ for some $\overline{b} \in U_p$. Then $\overline{a}^{(p-1)/2} = \left(\overline{b}^2\right)^{(p-1)/2} = \overline{b}^{p-1} = 1$ by Theorem 2.9.

But there are $(p-1)/2$ quadratic residues, and $x^{(p-1)/2}-1$ has degree $(p-1)/2$. So the roots of $x^{(p-1)/2}-1$ are exactly the quadratic residues modulo p, by Proposition 4.5.

Therefore, the quadratic non-residues must all be roots of $x^{(p-1)/2}+1$. In other words, if $\overline{a}$ is a quadratic non-residue then $\overline{a}^{(p-1)/2} = \overline{-1}$.

In either case, we have $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$. □

Proposition 6.4. *Let p be an odd prime. Suppose* $\gcd(ab, p) = 1$. *Then*

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

Proof. Certainly,

$$(ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2}.$$

By Proposition 6.3,

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

But since p is odd, $-1 \not\equiv 1 \bmod p$ so it must be that

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

(since each side is either ± 1 and they are congruent modulo p). □

The goal of this chapter is to look at quadratic reciprocity. Here is a preview.

Proposition 6.5. *Let p be an odd prime. Then*

$$\left(\frac{a}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} -1 & \text{if } p \equiv 3 \bmod 4 \\ 1 & \text{if } p \equiv 1 \bmod 4 \end{cases}$$

Proof. By Proposition 6.3, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Now, if $p \equiv 1 \bmod 4$ then this is 1 and if $p \equiv 3 \bmod 4$ then this is -1. □

Remark 6.6. We see clearly that the value of $\left(\frac{a}{p}\right)$ depends on $a \bmod p$. But Proposition 6.5 tells us that the value of $\left(\frac{a}{p}\right)$ may depend on the congruence class of p modulo an integer depending on a. For example, $(-1/p)$ depends on p modulo 4.

Later, quadratic reciprocity will tell us that $\left(\frac{a}{p}\right)$ will depend on $p \bmod 4a$.

Proposition 6.7. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases}$$

Proof. We have that $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right)$ by Proposition 6.3. The idea is to look at the sequence

$$2, 4, 6, \ldots, (p-1).$$

On one hand, the product of the terms is

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^{(p-1)/2} \cdot 1 \cdot 2 \cdots (p-1)/2.$$

We will calculate the product modulo p in another way.

First, let $2i$ be given where $1 \leq i \leq (p-1)/2$. Then we claim that there exists $1 \leq s_i \leq (p-1)/2$ and $\epsilon_i = \pm 1$ such that $2i \equiv \epsilon_i s_i \bmod p$. Indeed, if $2i \leq (p-1)/2$ then $s_i = 2i$ and $\epsilon_i = 1$ and if $(p-1)/2 < 2i \leq (p-1)$ then $2i \equiv -(p-2i) \bmod p$ so take $s_i = p-2i$ and $\epsilon_i = -1$.

Therefore,

$$2 \cdot 4 \cdot 6 \cdots (p-1) = \prod_{i=1}^{(p-1)/2} \epsilon_i s_i.$$

Now, we claim $s_1, s_2, \ldots, s_{(p-1)/2}$ is a permutation of $1, 2, \ldots, (p-1)/2$.

It is enough to show that if $2i \equiv \pm 2j \bmod p$ with $1 \leq i, j \leq (p-1)/2$ then $i = j$. Since p is odd, we have $i \equiv \pm j \bmod p$. Then p divides either $i-j$ or $i+j$. But $-(p-1)/2 \leq i-j \leq (p-1)/2$ and the only multiple of p in that range is 0 so $i = j$.

Similarly if p divides $i+j$ we have $2 \leq i+j \leq (p-1)$ and there are no multiples of p in this range. So it must be that $i = j$.

Finally, we can complete the proof. We have that

$$2^{(p-1)/2} \equiv \prod_{i=1}^{(p-1)/2} \epsilon_i,$$

and $\epsilon_i = -1$ if and only if $2i > (p-1)/2$.

So if the number of i such that $2i > (p-1)/2$ is odd, then $2^{(p-1)/2} \equiv -1 \bmod p$.

Look: $p-1, (p-3), \ldots, (p+1-2j) > (p-1)/2$.

But then $2p+2-4j > p-1$ so $p-4j+3 > 0$.

Therefore, solve $1 \leq 4j < p+3$. How many solutions are there? There are $(p+1)/4$ of them if $p \equiv 3, 7 \bmod 8$. This is an odd number if $p \equiv 3 \bmod 8$ and an even number if $p \equiv 7 \bmod 8$

There are $(p-1)/4$ of them if $p \equiv 1, 5 \bmod 8$. This is an even number if $p \equiv 1 \bmod 8$ and an odd number if $p \equiv 5 \bmod 8$.

So we have now established the formula that

$$\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \bmod 8 \\ 1 & \text{if } p \equiv \pm 1 \bmod 8 \end{cases}$$

It remains to see that $(p^2-1)/8$ is even if and only if $p \equiv \pm 1 \bmod 8$ (exercise). $\square$

In the proof of Proposition 6.7, there is a calculation we can extract.

Proposition 6.8. *Let p be an odd prime, and let $a \in U_p$. Consider the sequence $a, 2a, 3a, \ldots, \frac{p-1}{2}a$. Let j be the number of elements in the sequence congruent to an integer $-s$ with $1 \leq s \leq (p-1)/2$. Then $\left(\frac{a}{p}\right) = (-1)^j$.*

Proof. Omitted. □

Theorem 6.9. *Let p, q be odd primes. Then*

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

Proof. Consider the set

$$W = \{(a,b) \mid 1 \leq a \leq \frac{q-1}{2}, 1 \leq b \leq \frac{p-1}{2}\}.$$

To compute $\left(\frac{p}{q}\right)$ we count the number of s with $1 \leq s \leq \frac{q-1}{2}$ and $ap \equiv -s \bmod q$ for some $1 \leq a \leq \frac{q-1}{2}$. Rewrite this equation as $ap - bq = -s$ for some integer b. We now claim that $(a,b) \in W$.

Certainly $1 \leq a \leq \frac{q-1}{2}$ and $b > 0$. Now, $bq = ap + s$ so $b = \frac{ap+s}{q} \leq p \cdot \frac{q-1}{2q} + \frac{q-1}{2q} < \frac{p+1}{2}$. Therefore, $b \leq \frac{p-1}{2}$ since b is an integer and p is odd.

So the number of s with $1 \leq s \leq \frac{q-1}{2}$ and $ap \equiv -s \bmod q$ for some $1 \leq a \leq \frac{q-1}{2}$ is equal to the number of elements (a,b) of W such that $-\frac{q-1}{2} \leq ap - bq \leq -1$, let this number be M.

So we have $\left(\frac{p}{q}\right) = (-1)^M$.

Similarly, $\left(\frac{q}{p}\right) = (-1)^N$ where N is the number of elements of the set

$$\{(a,b) \in W \mid 1 \leq ap - bq \leq \frac{p-1}{2}\}.$$

In total the number of elements of W is $\frac{p-1}{2}\frac{q-1}{2}$. The leftover elements are the two sets

$$\{(a,b) \in W \mid ap - bq \leq -\frac{q+1}{2}\}$$

and

$$\{(a,b)|inW \mid ap - bq \geq \frac{p+1}{2}\}.$$

We claim that these two sets have the number of elements, say R.

If this is true, then the theorem follows since $\frac{p-1}{2}\frac{q-1}{2} = N + M + 2R$ and so

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

Now, the two sets above are in one-to-one correspondence: if $ap - bq \leq -\frac{q+1}{2}$ then let $a' = \frac{q+1}{2} - a$ and $b' = \frac{p+1}{2} - b$ and then

$$a'p - b'q = -(ap - bq) + \frac{(q+1)p - (p+1)q}{2} = -(ap - bq) + \frac{p-q}{2}$$

from which you can see that $a'p - b'q \geq \frac{p+1}{2}$. Details are omitted. □

7. Continued fractions

Definition 7.1. A simple continued fraction is an expression of the form

$$c = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}$$

where $a_0 \in \mathbb{Z}$ and $a_1, \ldots, a_n$ are positive integers. We write $c = [a_0; a_1, \ldots, a_n]$.

Note that if $\alpha = [a_0; a_1, \ldots, a_n]$ is a simple continued fraction and $a_n > 1$ then also $\alpha = [a_0; a_1, \ldots, a_n - 1, 1]$ as well.

Definition 7.2. Let $a_0 \in \mathbb{Z}$, $a_1, \ldots, a_n$ positive integers and $\alpha > 1$. Then a nearly simple continued fraction is an expression

$$c = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n + \frac{1}{\alpha}}}}}$$

and we use the notation $c = [a_0; a_1, \ldots, a_n, \alpha]$.

‘

Definition 7.3. Suppose $c = [a_0; a_1, a_2, \ldots, a_n, \alpha]$ is a nearly simple continued fraction for c. Then the n-th convergents to c are defined to be the integers p_n, q_n such that $q_n > 0$, $\gcd(p_n, q_n) = 1$ and

$$[a_0; a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}.$$

We have $p_0 = a_0$ and $q_0 = 1$, $p_1/q_1 = a_0 + 1/a_1 = (a_1a_0 + 1)/a_1$, etc.

Proposition 7.4. *For all $\alpha > 0$, we have*

$$[a_0; a_1, \ldots, a_n, \alpha] = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}$$

Proof. (By induction). Assume that

$$[a_0; a_1, \ldots, a_{n-1}, \alpha] = \frac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}$$

for all $\alpha > 0$. Then taking $\alpha = a_n$ gives the formula

$$\frac{p_n}{q_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}.$$

Now,

$$\begin{aligned}
[a_0; a_1, \ldots, a_{n-1}, a_n, \alpha] &= [a_0; a_1, \ldots, a_{n-1}, a_n + \alpha^{-1}] \\
&= \frac{(a_n + \alpha^{-1})p_{n-1} + p_{n-2}}{(a_n + \alpha^{-1})q_{n-1} + q_{n-2}} \\
&= \frac{a_n p_{n-1} + p_{n-2} + \alpha^{-1} p_{n-1}}{a_n q_{n-1} + q_{n-2} + \alpha^{-1} q_{n-1}} \\
&= \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}
\end{aligned}$$

as required. □

Proposition 7.5. *We have*

$$p_{n+1} = a_n p_n + p_{n-1}$$

and

$$q_{n+1} = a_n q_n + q_{n-1}$$

for all $n \geq 1$.

Proof. See proof of Proposition 7.4. □

Proposition 7.6. *Let* $x \in \mathbb{Q}$. *Then we can write* $x = [a_0; a_1, \ldots, a_n]$ *for some integer* a_0 *and positive integers* $a_1, \ldots, a_n$.

Proof. Let $x = a_0 + a/b$ where $a_0 \in \mathbb{Z}$ and $0 < p/q < 1$. Write $b = q_0 a + r_0$. Then

$$x = a_0 + \frac{1}{q_0 + (r_0/a)}$$

Now, write $a = q_1 r_0 + r_1$. Then

$$x = a_0 + \frac{1}{q_0 + \frac{1}{q_1 + r_1/r_0}}$$

and applying the Euclidean algorithm, eventually we are writing

$$r_{n-1} = q_{n+1} r_n + 0,$$

with the result that

$$x = a_0 + \cfrac{1}{q_0 + \cfrac{1}{q_1 + \cfrac{1}{\ddots + \cfrac{1}{q_{n+1}}}}}$$

so that $x = [a_0; q_0, q_1, \ldots, q_{n+1}]$ as required. □

Proposition 7.7. *We have*

$$p_{n+1}q_n - p_n q_{n+1} = (-1)^n.$$

Proof. We have $p_0 = a_0$, $q_0 = 1$ and $p_1 = a_0a_1 + 1$, $q_1 = a_1$. And

$$(a_1a_0 + 1) \cdot 1 - a_0a_1 = 1 = (-1)^0$$

Now, assume that $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$. Consider

$$\begin{aligned} p_{n+1}q_n - p_nq_{n+1} &= (a_{n+1}p_n + p_{n-1})q_n - p_n(a_{n+1}q_n + q_{n-1}) \\ &= p_{n-1}q_n - p_nq_{n-1} \\ &= -(-1)^{n-1} = (-1)^n \end{aligned}$$

completing the proof by induction. □

Proposition 7.8. *We have*

$$\left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_nq_{n-1}}.$$

Proof. Consider

$$\begin{aligned} \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| &= \left|\frac{(-1)^n}{q_nq_{n-1}}\right| \\ &\leq \frac{1}{q_nq_{n-1}}. \end{aligned}$$

□

Theorem 7.9. *Let $c_n = p_n/q_n$ be the convergents for the real number α. Then*

$$\begin{aligned} c_0 < c_2 < c_4 < \cdots < c_{2n} < \cdots < \alpha \\ < \cdots < c_{2n+1} < \cdots < c_5 < c_3 < c_1. \end{aligned}$$

Furthermore, $\lim_{n\to\infty} c_n = \alpha$.

Proof. Certainly $c_0 < \alpha < c_1$.

Suppose now that $c_n < \alpha < c_{n+1}$. Let $f(z) = \frac{p_n + zp_{n+1}}{q_n + zq_{n+1}}$. Then $f'(z) > 0$ on the interval $[0, \infty)$.

Notice that $f(a_{n+2}) = c_{n+2}$. Also,

$$\begin{aligned}\frac{p_{n+3}}{q_{n+3}} &= \frac{a_{n+3}p_{n+2} + p_{n+1}}{a_{n+3}q_{n+2} + q_{n+1}} \\ &= \frac{a_{n+3}(a_{n+2}p_{n+1} + p_n) + p_{n+1}}{a_{n+3}(a_{n+2}q_{n+1} + q_n) + q_{n+1}} \\ &= \frac{a_{n+3}p_n + (a_{n+2}a_{n+3} + 1)p_{n+1}}{a_{n+3}p_n + (a_{n+2}a_{n+3} + 1)q_{n+1}} \\ &= f\left(\frac{a_{n+2}a_{n+3} + 1}{a_{n+3}}\right)\end{aligned}$$

Furthermore, $f(0) = c_n$ and $f(z) \to c_{n+1}$ as $z \to \infty$.

Roughly $c_n < c_{n+2} = f(a_{n+2}) < f(\alpha_{n+2}) < f(\cdots) = c_{n+3} < c_{n+1}$ and $f(\alpha_{n+2}) = \alpha$.

Now, applying Proposition 7.8 implies that $\lim_{n\to\infty} c_n = \alpha$. □

Definition 7.10. A continued fraction $\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]$ is called eventually periodic if there exists an integer N and an integer k such that

$$a_{n+k} = a_n \text{ for all } n \geq N.$$

A continued fraction $\alpha = [a_0; a_1, \ldots, a_n, \ldots]$ is called purely periodic if there exists an integer k such that $a_{n+k} = a_n$ for all $n \geq 0$.

Theorem 7.11. *Let $\alpha = [\overline{a_0, a_1, \ldots, a_k}]$ be a purely periodic continued fraction. Then α is the root of a quadratic equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{Z}$. Furthermore, if $\beta = [\overline{a_k, a_{k-1}, \ldots, a_0}]$ then $\alpha' = -1/\beta$ and $-1 < \alpha' < 0$ is the conjugate root to α of $ax^2 + bx + c = 0$.*

Conversely, if α is the root of a quadratic equation $ax^2 + bx + c = 0$ and $\alpha > 0$ and the conjugate root α' lies between -1 and 0 then α is purely periodic.

Proof. Omitted. □

Theorem 7.12. *Let $N > 0$ be a square-free integer. Then*

$$\sqrt{N} = [a, \overline{a_1, a_2, \ldots, a_i, a_i, \ldots, a_2, a_1, 2a}]$$

or

$$\sqrt{N} = [a, \overline{a_1, a_2, \ldots, a_i, a_{i-1}, \ldots, a_2, a_1, 2a}]$$

Proof. There exists $a \in \mathbb{Z}$ such that $a + \sqrt{N}$ is a purely periodic quadratic irrational. Write $a + \sqrt{N} = [\overline{a_0, a_1, \ldots, a_k}]$. Then if $\beta = [\overline{a_k, a_{k-1}, \ldots, a_0}]$ we have $-1/\beta = a - \sqrt{N}$ so $1/\beta = \sqrt{N} - a$. But $1/\beta = [0, \overline{a_k, a_{k-1}, \ldots, a_0}]$ and $\sqrt{N} = [a, \overline{a_k, \ldots, a_0}]$. But also, $\sqrt{N} =$

$[a_0 - a, a_1, \ldots, a_k, a_0, a_1, \ldots]$ This implies $a_0 = 2a$, $a_k = a_1, a_2 = a_{k-1}, \ldots$ So the continued fraction of $\sqrt{N}$ is

$$\sqrt{N} = [a, \overline{a_1, a_2, \ldots, a_i, a_i, \ldots, a_2, a_1, 2a}]$$

or

$$\sqrt{N} = [a, \overline{a_1, a_2, \ldots, a_{i-1}, a_i, a_{i-1}, \ldots, a_2, a_1, 2a}]$$

□

8. Pell equations

Definition 8.1. Let $N > 0$ be a square-free integer. Then the equation

$$x^2 - Ny^2 = 1$$

is called a Pell's equation, and

$$x^2 - Ny^2 = -1$$

is called a negative Pell's equation.

Proposition 8.2. *Let* $\sqrt{N} = [a, \overline{a_1, a_2, \ldots, a_2, a_1, 2a}]$ *and let*

$$p_n/q_n = [a, a_1, a_2, \ldots, a_2, a_1].$$

Then

$$p_n^2 - Nq_n^2 = (-1)^n.$$

Proof. Omitted. □

9. Cryptography and RSA

Let us try to describe the goal of cryptography. Imagine two people want to communicate sensitive information. In cryptography, these people are called Alice and Bob. But they can only communicate over an insecure channel. For example, maybe they are broadcasting their message by using a radio, or they are communicating on a message board. Or, maybe they are communicating over the internet and they are worried that some actor may intercept their message. It is unacceptable for them to send their messages directly.

So Alice wants to send Bob a message and she wants to make sure that no one except for Bob can decode the message. First, Alice converts her message into a positive integer, say m. Then Alice performs some transformation on m, and obtains a ciphertext c (also an integer). Alice sends c to Bob. Bob receives c and needs to be able recover m.

The requirements on the transformation that Alice uses are:

a) it shouldn't take too long to compute c given m
b) Similarly, c shouldn't take up much more space than m.

c) When Bob receives c, he should be able to recover m without much trouble
d) But if an undesirable actor intercepts c, they should not be able to recover m.

In this chapter, we will describe the RSA public-key cryptography system.

Definition 9.1. This is how Bob chooses a private key and public key in RSA.

a) Bob chooses two prime numbers p and q.
b) Bob computes $N = pq$ and $\phi(N) = (p-1)(q-1)$.
c) Bob chooses a secret key d such that $1 < d < \phi(N)$ and such that $\gcd(d, \phi(N)) = 1$.
d) Bob computes e with $1 < e < \phi(N)$ such that $ed \equiv 1 \bmod \phi(N)$.

Now, Bob's public key is defined to be (N, e). Bob's private key is defined to be $(\phi(N), d)$.

Definition 9.2. Alice has a message $m \in \mathbb{Z}/N\mathbb{Z}$ and she wants to send the message safely to Bob. She looks up Bob's public key: (N, e). She computes $\overline{c} = \overline{m}^e \in \mathbb{Z}/N\mathbb{Z}$.

Definition 9.3. Bob receives the ciphertext c from Alice. He computes $\overline{c}^d \in \mathbb{Z}/N\mathbb{Z}$.

Proposition 9.4. *Let $\overline{c} = \overline{m}^e \in \mathbb{Z}/N\mathbb{Z}$. Then $\overline{c}^d = \overline{m}$.*

So when Bob decrypts c by computing $\overline{c}^d$ using his private-key, he has successfully recovered the original message m.

Proof. We have $de \equiv 1 \bmod \varphi(N)$. Therefore, $\overline{c}^d = (\overline{m}^e)^d = \overline{m}^{de} = \overline{m}^{1+k\varphi(n)} = \overline{m}$ by Theorem 2.11. □

Proposition 9.5. *Let $\overline{x} \in \mathbb{Z}/N\mathbb{Z}$ and n be a positive integer. There is an algorithm that can compute $\overline{x}^n$ in approximately $\log n$ steps.*

Proof. Here, we just give the algorithm. We are given n and $\overline{x} \in \mathbb{Z}/N\mathbb{Z}$.

a) initialize $r = \overline{1}$
b) write $n = 2n' + b$
c) set $r \leftarrow r \cdot x^b$
d) set $r \leftarrow r^2$ and $n \leftarrow n'$
e) if $n' = 0$ then stop, otherwise go to step 2.

□

10. Elliptic curves over the rationals

Definition 10.1. For us, an elliptic curve over $\mathbb{Q}$ will be a cubic equation of the form

$$E: \ y^2 = x^3 + Ax + B,$$

where A, B are rational numbers.

Let $f(x) = x^3 + Ax + B$. We require that $f(x)$ has three distinct roots in $\mathbb{C}$.

Definition 10.2. The rational points of E, denoted $E(\mathbb{Q})$, is

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Here ∞ means 'the point at infinity'.

Proposition 10.3. *Let $P, Q \in E(\mathbb{Q})$ be two distinct points and suppose $P, Q \neq \infty$. Then there exists a third point $R \in E(\mathbb{Q})$ which is collinear with P, Q.*

Proof. If the line intersecting P, Q is a vertical line, let $R = \infty$.

Otherwise, let $y = mx + b$ be the line joining P and Q. Then substitute this equation into the equation for E:

$$(mx + b)^2 = x^3 + Ax + B.$$

This equation has two roots corresponding to the x-coordinates of P, Q. Let the third root be x_0. Then $x_0 \in \mathbb{Q}$ (since the other two roots are rational). Then $y_0 = mx_0 + b \in \mathbb{Q}$ as well and $R = (x_0, y_0)$ is the point we are looking for. □

Proposition 10.4. *Let $P \in E(\mathbb{Q})$ and $P \neq \infty$. Then the tangent line to E at P intersects E at a point $R \in E(\mathbb{Q})$.*

Proof. Find the slope of the tangent line to E at $P = (a, b)$. Use implicit differentiation:

$$2 \ dy \ b = 3a^2 \ dx \ + A \ dx$$

at the point $P = (a, b)$:

$$\frac{dy}{dx} = \frac{3a^2 + A}{2b},$$

unless $b = 0$. If $b = 0$ then the tangent line is $x = a$, and we take $R = \infty$.

Otherwise, set $m = \frac{3a^2+A}{2b}$ and substitute $b = \frac{3a^2+A}{2b}a + c$.

$$c = \frac{-b^2 + 3B}{2b}$$

So the tangent line is $y = \frac{3a^2+A}{2b}x + \frac{-b^2+3B}{2b}$. This line intersects E at a third point since $x = a$ is a double root. Let R be the third point (just as in Proposition 10.3). □

Definition 10.5. Let $P \in E(\mathbb{Q})$. Define $-P \in E(\mathbb{Q})$ to be

a) ∞ if $P = \infty$
b) $(a, -b)$ if $P = (a, b)$

Let $P, Q \in E(\mathbb{Q})$.
Define $P + Q \in E(\mathbb{Q})$ as

a) If $P = \infty$ then define $P + Q = Q$
b) If $P = Q$, let R be as in Proposition 10.4, and define $2P = -R$
c) If $P \neq Q$, let R be as in Proposition 10.3 and define $P + Q = -R$.

Theorem 10.6. *The set $E(\mathbb{Q})$ with composition defined by Definition 10.5 is an abelian group.*

Proof. Omitted. □

Theorem 10.7. *There is an integer $r \geq 0$ and points $P_1, \ldots, P_r$ which generate $E(\mathbb{Q})$ as an abelian group.*

Proof. Omitted. □

Definition 10.8. We can write

$$E(\mathbb{Q}) \cong (\mathbb{Z})^r \oplus A$$

where A is a finite abelian group. (In fact, a lot is known of the structure of A).

Then r is called the rank of E. If $r = 0$ then E has finitely many rational points and if $r > 0$ then E has infinitely many points.

Definition 10.9. Let n be a positive integer. Then n is called a congruent number if it is the area of a right triangle with rational side lengths.

Proposition 10.10. *Let n be an integer. Let $E_n : y^2 = x^3 - n^2x$. Let r_n be the rank of E_n. Then n is a congruent number if and only if the rank of E_n is positive.*

Proof. We will just prove that if $r_n > 0$ then n is a congruent number. The converse is more difficult and we will omit it.

Let $P = (a, b)$ be a point of infinite order on $E_n(\mathbb{Q})$. We have $b \neq 0$ (else, $2P = 0$). Furthermore, we may assume that $a > 0$. (This can be seen if you draw a picture of the real points of E).

Now, let $A = \frac{a^2-n^2}{b}$, $B = \frac{2na}{b}$, $C = \frac{a^2+n^2}{b}$.

We claim that $A^2 + B^2 = C^2$ and $\frac{AB}{2} = n$. (Check it). □

References

[Fla18] Daniel E. Flath. *Introduction to number theory*. With errata, Reprint of the 1989 edition. AMS Chelsea Publishing, Providence, RI, 2018, pp. xii+212.