Elementary Number Theory in 40 Days with Prof. Allen

Yün Han

Thanks to Prof. Patrick Allen for his unsurpassed inspirational teaching.

Contents

Preface

This book is based on the notes I took while sitting in Prof. Patrick Allen's lectures of Math 453 in Spring 2017. Each lecture was around 50 minutes and the term started on 17 January and ended on 3 May.

The format of the course included lectures on Monday, Wednesday and Friday every week; one office hours each Monday; one homework session each Wednesday; two midterms (on 24 February and 31 March each) and one final (on 5 May). Weekly homework and reflection was assigned every Friday.

On top of the lecture notes, I also added reading notes that were not in the original lectures. Most included exercise problems are from *100 Problems in Elementary Number Theory* by Ko Chao [**Ko80**].

This book can be used as a companion to *Elementary Number Theory* by James Strayer [**Str01**] or a self-study guide.

Champaign, Illinois, 2017 Yün Han

Part 1

January to February, 2017

LECTURE 1

Day One

— 18.01.2017

[1]Recall the set of integers

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

We ask the following questions:

- Does 2 divide 6 in $\mathbb{Z}$? (Yes.)
- Does 6 divide 2 in $\mathbb{Z}$? (No.)
- Does 0 divide 0 in $\mathbb{Z}$? (Yes.)

Definition 1.1. Let a, b be integers. We say that b **divides** a, written as $b \mid a$ if there is an integer c such that $a = bc$. And b is called a **divisor** of a; otherwise $b \nmid a$.

For the above preceding questions,

- $2 \mid 6$ since $6 = 3 \times 2$. Both 3 and 2 are integers.
- $6 \nmid 2$ since there is no $c \in \mathbb{Z}$ such that $2 = 6c$.
- $0 \mid 0$ since for $\forall\ c \in \mathbb{Z}$, we have $0 = 0c$.

Proposition 1.2. *Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. Since $a \mid b$, we have $\exists\ d \in \mathbb{Z}$ such that $b = ad$. Similarly, $\exists\ e \in \mathbb{Z}$ such that $c = be$. Then $c = (ad)e = a(de)$ and de is an integer. By the definition of divisibility, $a \mid c$. □

Proposition 1.3. *Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then for any $m, n \in \mathbb{Z}$, we have $c \mid (am + bn)$.*

Proof. $c \mid a$ implies $\exists\ d \in \mathbb{Z}$ such that $a = cd$. $c \mid b$ implies $\exists\ e \in \mathbb{Z}$ such that $b = ce$. For any $m, n \in \mathbb{Z}$,

$$\begin{aligned} am + bn &= (cd)m + (ce)n \\ &= c(dm) + c(en) \\ &= c(dm + en), \end{aligned}$$

where $dm + en$ is a linear combination of d, e with integer coefficients m, n. (i.e., $dm + en \in \mathbb{Z}$.) Therefore $c \mid (am + bn)$. □

Theorem 1.4 (Division algorithm). *Let $a, b \in \mathbb{Z}$, $b > 0$. There are* ***unique*** *integers $q, r \in \mathbb{Z}$, such that $a = qb + r$ with $0 \leqslant r < b$.*

Proof. To prove the existence of such q and r, consider the rational number $\frac{a}{b}$. (Our assumption $b > 0$ implies $b \neq 0$.) Let q be the largest integer less than $\frac{a}{b}$, denoted as $q = \lfloor \frac{a}{b} \rfloor$.

Let $r = a - qb$. The range of r is $0 \leqslant r < b$.

- $r = a - qb \geqslant 0$. Indeed, since $q \leqslant \frac{a}{b}$ and $b > 0$, we have $qb \leqslant a$, i.e., $a - qb \geqslant 0$.
- $r < b$, otherwise if $r \geqslant b$, $r = a - qb \geqslant b$. Further it implies $a \geqslant (q+1)b$, so $\frac{a}{b} \geqslant q + 1$, which contradicts the fact that q is the largest integer such that $q \leqslant \frac{a}{b}$. (Now $q + 1$ is an integer such that $q < q + 1 \leqslant \frac{a}{b}$ if $r \geqslant b$.)

[1] Text of Math 453: *Elementary Number Theory* by J. Strayer [**Str01**].

Hence the proof of existence.

To prove the uniqueness of such q and r, let $q', r' \in \mathbb{Z}$, such that $a = q'b + r'$ with $0 \leqslant r' < b$.

We want to show that $q' = q$, and $r' = r$. Since $r' \geqslant 0$, we have $0 \leqslant r' = a - q'b \implies a \geqslant q'b$. So $\frac{a}{b} \geqslant q'$ by $b > 0$. Since $r' < b$, we have $a = q'b + r < q'b + b \implies a < (q'+1)b$. It further implies $\frac{a}{b} < q' + 1$. Therefore, we showed q' is also the largest integer bounded by $\frac{a}{b}$. Hence $q' = \lfloor \frac{a}{b} \rfloor = q$.

$r' = r$ follows from the fact that $r' = a - q'b = a - qb = r$. □

Exercise.

1.1. Let $m, n \in \mathbb{Z}$ with $m, n > 0$. Show that

$$\frac{1}{m} + \frac{1}{m+1} + \cdots + \frac{1}{m+n}$$

is not an integer.

1.2. Let $\alpha \in \mathbb{Q}$. Let b be the smallest positive integer such that $b\alpha$ is an integer. If there is a $c \in \mathbb{Z}$ such that $c\alpha$ is an integer, then $b \mid c$.

1.3. Let $k, n \in \mathbb{Z}$, $n > 1$. Let $m = 2^{n-1}(2^n - 1)$. Show that any $1 \leqslant k \leqslant m$ can be written as $k = \sum_{d \mid m} \ell d$, where $\ell = 0$ or 1, d is a divisor of m.

1.4. Let $a, b \in \mathbb{Z}$ with $a > 0$, $b > 2$. Show $2^b - 1 \nmid a^a + 1$.

LECTURE 2

Day Two

— 20.01.2017

THEOREM 2.1 (Mathematical induction). *Let $m \in \mathbb{Z}$ and $\mathcal{S} \subseteq \mathbb{Z}$ satisfying*

- *$m \in \mathcal{S}$;*
- *If $k \geqslant m$ and $k \in \mathcal{S}$ then $k+1 \in \mathcal{S}$.*

Then all integers $n \geqslant m$ are in $\mathcal{S}$.

REMARK 2.2. Theorem 2.1 was stated without proof. The proof uses "well ordering property".

How to use this? Say we have a statement depending on integer $n \geqslant m$ that we want to prove true, then if we show it is

- Base case: true for $n = m$;
- Inductive step: also true for $k+1$ assuming true for arbitrary $k \geqslant m$.

Then the statement is true for all $n \geqslant m$.

EXAMPLE 2.3 (Bernoulli's inequality). Let $x > -1$ be a non zero real number. Then

$$(1+x)^n \geqslant 1 + nx$$

for all $n \geqslant 2$.

PROOF. We prove it by induction on $n \geqslant 2$.
First take $n = 2$. Then

$$\begin{aligned}(1+x)^2 &= 1 + 2x + x^2 \\ &\geqslant 1 + 2x. && \text{(by } x^2 \geqslant 0\text{)}\end{aligned}$$

Assume it is true for $n = k$, $k \geqslant 2$.

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x) \\ &= (1+x)^k + (1+x)^k x \\ &\geqslant 1 + kx + (1+kx)x && \text{(by induction hypothesis)} \\ &\geqslant 1 + kx + x && \text{(by } kx^2 \geqslant 0\text{)} \\ &= 1 + (k+1)x.\end{aligned}$$

By mathematical induction in Theorem 2.1, $(1+x)^n \geqslant 1 + nx$ for all $n \geqslant 2$. □

There is also a variant of mathematical induction called *strong induction*: Say we have a statement indexed by integers $n \geqslant m$ that we want to prove true. If we prove

- Base case: the statement is true for $n = m$;
- Inductive step: it is also true for $k+1$ assuming it is true for each of m, $m+1$, …, k given arbitrary $k \geqslant m$.

Then the statement is true for all $n \geqslant m$.

Let us go back to number theory.

DEFINITION 2.4. Let $p > 1$ be an integer. We say p is **prime** if its only divisors are 1 and p itself. An integer $n > 1$ is called **composite** if it is not prime.

PROPOSITION 2.5. *Any integer $n > 1$ is a product of primes.*

PROOF. We prove this by strong induction. When $n = 2$, n is prime, and it is a product of one prime 2 itself. Fix some $k \geqslant 2$ and assume any integer $2 \leqslant n \leqslant k$ is a product of primes. We want to show that $k + 1$ is also a product of primes.

If $k + 1$ is prime, then we are done; if $k + 1$ is not prime, then it is composite. Then $k + 1$ can be written as

$$k + 1 = ab,$$

where $1 < a < k + 1$ (or $2 \leqslant a \leqslant k$) and $1 < b < k + 1$ (or $2 \leqslant b \leqslant k$). By induction hypothesis, both a and b are a product of primes. Then $k + 1 = ab$ is a product of primes. Hence the proposition. □

THEOREM 2.6 (Fundamental theorem of arithmetic). *Any integer $n \geqslant 2$ can be written as $n = p_1 p_2 \cdots p_k$ with $p_1, p_2, \ldots, p_k$ primes.*[1] *This expression is* ***unique*** *up to an ordering.*

PROOF. The fundamental theorem of arithmetic (FTA) will be proved in Lecture 5. □

THEOREM 2.7 (Euclid). *There are infinitely many primes.*

PROOF. Assume the contrary, there are finitely many primes. Let $p_1, p_2, \ldots, p_k$ be all the primes, $k \in \mathbb{Z}$, $k > 0$. Consider the number $N = p_1 p_2 \cdots p_k + 1 = \left(\prod_{i=1}^k p_i\right) + 1$. By Proposition 2.5, for $N > 1$, N is a product of primes, i.e., there is a prime p such that $p \mid N$. But $p = p_i$ for some $1 \leqslant i \leqslant k$. Now we have $p_i \mid N$ and $p_i \mid \prod_{i=1}^k p_i$. By Proposition 1.3 from last lecture, we have

$$\begin{aligned} p_i \mid 1 \cdot N + (-1) \cdot \prod_{i=1}^k p_i &= \left(\prod_{i=1}^k p_i\right) + 1 - \prod_{i=1}^k p_i \\ &= 1. \end{aligned}$$

So $p_i \mid 1$ for some prime p_i, a contradiction. □

PROPOSITION 2.8. *Let $n > 1$ be composite. Then there is a prime divisor p of n with $p \leqslant \sqrt{n}$.*

PROOF. Since n is composite, we can write $n = ab$ for some $a, b \in \mathbb{Z}$, $1 < a < n$ and $1 < b < n$. Without loss of generality, assume $a \leqslant b$. Then $a \leqslant \sqrt{n}$. (Otherwise $ab > a \cdot a > \sqrt{n} \cdot \sqrt{n} = n$.)

Since $a > 1$, a has some prime divisor p with $p \leqslant a$ by Proposition 2.5. $p \mid a$ and $a \mid n$ imply $p \mid n$ by Proposition 1.2. $p \leqslant a \leqslant \sqrt{n}$. Therefore p is the prime divisor of n we are looking for. Hence such prime divisor of n exists. □

Exercises.

2.1. Let $n \in \mathbb{Z}$ and $n > 1$. Show that $n^5 + n^4 + 1$ is composite.

2.2. Find all $n \in \mathbb{Z}$, $n > 0$ such that $3^{2n+1} - 4^{n+1} + 6^n$ is prime. (*Hint*: $3x^2 + xy - 4y^2 = (3x + 4y)(x - y)$.)

2.3. Let p be a prime. Let $a \in \mathbb{Z}$ with $p \nmid a$. If b is the smallest positive integer such that $\frac{ba}{p}$ is an integer, then $b = p$.

2.4. Let $a_1 = a_2 = a_3 = 1$, $a_{n+1} = \dfrac{1 + a_n a_{n-1}}{a_{n-2}}$ for $n \geqslant 3$. Show that a_i is an integer for all $i \in \mathbb{Z}$, $i > 0$.

[1] Not necessarily distinct.

LECTURE 3

Day Three

— 23.01.2017

The immediate consequence of Proposition 2.8 in the last lecture is that: if an integer $n \geqslant 2$ has no divisors d for all $1 < d \leqslant \sqrt{n}$, then n is prime. This leads us to the *Sieve of Eratosthenes*, to find all primes bounded by a given integer n.

Algorithm (Sieve of Eratosthenes):

- Write down all integers i, $2 \leqslant i \leqslant n$;
- Start at 2: leave 2 but cross out all multiples of 2;
- Repeat, leaving the next non crossed out integer and cross out all its multiples;
- When the non crossed out integer is greater than $\sqrt{n}$, stop the process;
- The resulting table of non crossed out integers are exactly the primes bounded by n.

How do primes behave?

Look at the sequence of primes,

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

note the occurrences of primes that differ by 2, i.e.,

$$\{3, 5\}, \{5, 7\}, \{11, 13\}, \{17, 19\}, \{29, 31\}, \ldots$$

these are called *twin primes.*

Conjecture 3.1 (Twin prime conjecture). *There are infinitely many twin primes.*

For an integer $n \geqslant 1$, let p_n be the nth prime, e.g., $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$. Then the twin prime conjecture can be formulated as

$$p_{n+1} - p_n = 2$$

for infinitely many n.

Theorem 3.2 (Zhang[1], 2013). *There is a constant C such that*

$$p_{n+1} - p_n \leqslant C$$

for infinitely many n. We can take $C = 70,000,000$.

The above bound can be improved to 246. Philosophically, the difficulty of the problem is primes are the atoms of integers with respect to *multiplication* (i.e., thinking of the fundamental theorem of arithmetic). But the twin prime conjecture involves *additive* information (i.e., the +2 part) as well. In general, no relation between the divisors of n and divisors of $n + 2$ can be said.

Conjecture 3.3 (Goldbach's conjecture, 1742). *Every even integer $n > 2$ can be written as the sum of two primes.*

The best result so for as far as Goldbach's conjecture is concerned is from J. Chen.

[1] Zhang's proof was regarded a Cinderella story. He submitted his proof to *Ann. Math.* in 2013 while he had been a lecturer in an unknown college for years without a secure academic appointment. He also had had many odd jobs over the years including working part time in a Subway's sandwich shop and sleeping rough from time to time since he obtained his doctorate in maths more than twenty years before he made his name in the mathematics community. He was thought to begin his college education at the age of 25 and doctoral studies not until he almost turned 30. He has a truly unusual and uneven career path of a mathematician.

THEOREM 3.4 (Chen, 1973). *There is a constant m such that every even integer $n \geqslant m$ can be written either as a sum of two primes or as a sum of a prime and a number that is the product of two primes.*

THEOREM 3.5 (Montgomery–Vaughan, 1975). *The set of positive integers for which the Goldbach's conjecture fails has density zero, i.e., Goldbach's conjecture holds most of the time.*

REMARK 3.6. Montgomery–Vaughan does not imply the integers which fail the Goldbach's conjecture form a finite set.

CONJECTURE 3.7 (Weak Goldbach's conjecture). *Every odd integer $n \geqslant 7$ is the sum of three primes.*

REMARK 3.8. Goldbach's conjecture implies the weak Goldbach's conjecture. For odd $n \geqslant 7$, $n-3$ is even and $n-3 \geqslant 4 \geqslant 2$. Hence the word "weak".

THEOREM 3.9 (Vinogradov, 1937). *There is a constant m such that any odd integer $n \geqslant m$ is the sum of three primes.*

THEOREM 3.10 (Helfgott, 2013). *The weak Goldbach's conjecture is true.*

The consequence of the weak Goldbach's conjecture is that: every even integer $n \geqslant 4$ is the sum of at most four primes.

REMARK 3.11. All the theorems listed in this lecture are beyond the scope of this course and their proofs require heavy machinery from Analytic Number Theory (e.g., at least at the level of Math 531).

We notice that primes seem to get more spaced out on average.

PROPOSITION 3.12. *For any integer $n \geqslant 1$, we can find n consecutive composite numbers.*

PROOF. Consider the string of n consecutive integers,

$$(n+1)!+2,\ (n+1)!+3,\ \ldots,\ (n+1)!+(n+1).$$

Since $(n+1)! = 1 \cdot 2 \cdot \cdots \cdot (n+1)$, we have $k \mid (n+1)!$ for $k = 2, 3, \ldots, n+1$. Further $k \mid (n+1)! + k$ by Proposition 1.3 for $k = 2, 3, \ldots, n+1$.

Notice $1 < k < (n+1)! + k$ by[2] $k \leqslant n+1 \leqslant (n+1)! < (n+1)! + k$, it implies each of $(n+1)! + k$'s is composite. □

Exercise.

3.1. Let $n \in \mathbb{Z}$, $n \geqslant 2$. Show that there exists an arithmetic progression of n pairwise coprime composite numbers. (*Hint*: Let $p > n$ be an odd prime and let N be an integer such that $N \geqslant p-(n-1)n!$. Consider arithmetic progression $N!+p,\ N!+p+n!,\ \ldots,\ N!+p+(n-1)n!$.)

[2] Or by $(n+1)! > 0$, then $k + (n+1)! > k$.

LECTURE 4

Day Four

— 25.01.2017

A notation from analytic number theory. If f and g are two real valued functions on an interval $(a,\infty) \subseteq \mathbb{R}$, $a \in \mathbb{R}$, we say f and g are **asymptotic** if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

and write $f \sim g$. Heuristically, this means $f = g +$ error term or in the little-o notation,

$$f = g + o(g).$$

Let $\pi(x)$ be the number of primes that are bounded by x. If we define a set $\mathcal{P}$

$$\mathcal{P} := \{1 \leqslant p \leqslant x : p \text{ is prime}\},$$

then

$$\begin{aligned}\pi(x) &= \mathbf{card}(\mathcal{P}) \\ &= \#\{1 \leqslant p \leqslant x : p \text{ is prime}\} \\ &= |\{1 \leqslant p \leqslant x : p \text{ is prime}\}|.\end{aligned}$$

card(set), #set, and |set| all denote the cardinality or the number of elements, or the size of a set.

Example 4.1. $\pi(10) = 4$, $\pi(25) = 9$.

Theorem 4.2 (Prime number theorem). *Let $\pi(x)$ be the number of primes that are less than or equal to x. We have*

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

Remark 4.3. The logarithm $\log x$ in the statement is the natural logarithm. The proof is an application of complex analysis and will not be given in this course. However there is an elementary proof given by A. Selberg in 1949 [**AS49**] but it is winding and difficult.

Let us step back to our discussion of fundamental theorem of arithmetic.

Definition 4.4. Let $a, b \in \mathbb{Z}$, not both zero. The **greatest common divisor** of a and b is the largest divisor d such that $d \mid a$ and $d \mid b$. We write $d = \gcd(a,b)$. If $\gcd(a,b) = 1$, we say a and b are **coprime** or relatively prime.

Example 4.5. Quick examples.

- $\gcd(-12, 15) = 3$.
- Let $a \in \mathbb{Z}$, $a > 0$, then $\gcd(a, 0) = a$.
- Let $a \in \mathbb{Z}$, then $\gcd(a, 1) = 1$.
- Let $a \in \mathbb{Z}$ and p prime, then

$$\gcd(a,p) = \begin{cases} 1 & \text{if } p \nmid a, \\ p & \text{if } p \mid a. \end{cases}$$

Example 4.6. Let $a, b \in \mathbb{Z}$, not both zero and let $d = \gcd(a,b)$. Note that $\frac{a}{d}$ and $\frac{b}{d}$ are integers, not both zero either. Show $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.

PROOF. We need to show $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Assume otherwise, we can write

$$\frac{a}{d} = me, \ \frac{b}{d} = ne$$

for some $m, n, e \in \mathbb{Z}$ with $e > 1$. Then we have $a = m(de)$ and $b = n(de)$ with $de > 0$ a positive divisor of both a and b. Further $de > d \cdot 1 > d$, which contradicts the fact that d is the greatest common divisor of a and b. Hence we completed the proof. □

PROPOSITION 4.7. *Let $a, b \in \mathbb{Z}$, not both zero, then*

$$\gcd(a, b) = \min \{ax + by : ax + by > 0, \forall\ x, y \in \mathbb{Z}\}.$$

PROOF. Let $\mathcal{S} = \{ax + by : ax + by > 0, \forall\ x, y \in \mathbb{Z}\}$. First we notice that $\mathcal{S}$ is nonempty. Indeed, a and b are not both zero, at least one of $\pm a$, $\pm b$ is positive, i.e., at least one of them belongs to $\mathcal{S}$. By well ordering property of a nonempty set $\mathcal{S}$, it has a minimal element. Call this minimum d. Since $d \in \mathcal{S}$, there exist $m, n \in \mathbb{Z}$ such that $d = am + bn$.

Let us show $d \mid a$ and $d \mid b$. By division algorithm (See Theorem 1.4), there exist unique $q, r \in \mathbb{Z}$ with $0 \leqslant r < d$ such that

$$a = dq + r.$$

Notice

$$\begin{aligned} r &= a - dq \\ &= a - (am + bn)q \\ &= a(1 - mq) + b(-nq). \end{aligned}$$

If $r > 0$, then $r \in \mathcal{S}$. But $r < d$ which contradicts the fact d is the minimum of $\mathcal{S}$. So $r = 0$. Hence $d \mid a$. Similar argument can be said about $d \mid b$. We proved d is a common divisor of a and b.

Next we show d is the greatest common divisor. Let $c \in \mathbb{Z}$, $c > 0$ be any common divisor of a and b. We need to show $c \leqslant d$. Indeed, $c \mid a$ and $c \mid b$ imply $c \mid am + bn = d$. Both c and d are positive and c is a divisor of d, i.e., $d = ce$ for some $e \in \mathbb{Z}$, $e > 0$. Hence $c \leqslant d$. □

PROPOSITION 4.8. *Let $a, b, p \in \mathbb{Z}$ with p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

PROOF. If $p \mid a$, we are done. We may assume $p \nmid a$ and we want to show $p \mid b$. By Example 4.5, $p \nmid a \implies \gcd(a, p) = 1$. By Proposition 4.7, there are $m, n \in \mathbb{Z}$ such that

$$\begin{aligned} 1 &= \gcd(a, p) \\ &= am + pn. \end{aligned} \tag{4.1}$$

Multiply Equation (4.1) by b on both sides, we have $b = (ba)m + p(bn)$. pbn is a multiple of p, further by our assumption, $p \mid ab$, so $p \mid b$ as desired. □

COROLLARY 4.9. *Let p be prime and let $a_1, a_2, \dots, a_k \in \mathbb{Z}$ for some $k \geqslant 1$. If $p \mid \prod_{i=1}^{k} a_i$, then $p \mid a_i$ for some $1 \leqslant i \leqslant k$.*

SKETCH OF PROOF. We induct on k. The rough idea is to group the product $a_1 a_2 \cdots a_{k+1}$ as $(a_1 a_2 \cdots a_k) a_{k+1}$, so we can treat this product as if the product is the multiplication of two terms. Then apply Proposition 4.8 which handles the case of product of exactly two terms. Check out [**Str01**, §1.5, Corollary 1.15] for details. ■

EXAMPLE 4.10. Let $p \in \mathbb{Z}$ with $p > 1$. p satisfies the following property,

$$\forall\ a, b \in \mathbb{Z} \text{ such that } p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Show p is prime.

PROOF. [1] Assume the contrary, p is composite. Then $p = mn$ for some $1 < m < p$, $1 < n < p$, $m, n \in \mathbb{Z}$. By the assumption, whenever $p \mid ab$ we have either $p \mid a$ or $p \mid b$. Swap a for b if necessary, we may assume $p \mid ab \implies p \mid a$.

Take $a = m$ and $b = n$ in our case. Then $p \mid m \implies m = pc$ for some integer c. But $p = mn = pcn$, it follows that $c = n = 1$ while $n > 1$, a contradiction. □

REMARK 4.11. This example gives an alternative definition of a prime.

Exercise.

4.1. Let $a, b \in \mathbb{Z}\backslash\{0, 1\}$. Show there exists $c \in \mathbb{Z}\backslash\{0, 1\}$ such that $\gcd(c, a) = \gcd(c, b) = 1$. (*Hint*: Assume $a, b > 0$ and take $c = ab + 1$.)

4.2. Let $m, n \in \mathbb{Z}$, $m, n > 0$ with m odd. Show $\gcd(2^m - 1, 2^n + 1) = 1$.

4.3. Let $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, $a + b \neq 0$. Let p be an odd prime. Show that

$$\gcd\left(a + b, \frac{a^p + b^p}{a + b}\right) = 1 \text{ or } p.$$

4.4. Let $a, b \in \mathbb{Z}$, $a, b > 0$ such that $ab + 1 \mid a^2 + b^2$. Show $\frac{a^2+b^2}{ab+1}$ is a perfect square.

4.5. Let $n \in \mathbb{Z}$, $n > 0$. Compute $\gcd\left(\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}\right)$.

[1] Left as an exercise, proof was not given in the lecture.

LECTURE 5

Day Five

— 27.01.2017

Fundamental theorem of arithmetic (FTA)

THEOREM 5.1 (Fundamental theorem of arithmetic). *Any integer $n \geqslant 2$ can be written as a product of primes*

$$n = p_1 p_2 \cdots p_k,$$

where k is a positive integer, and this expression is unique up to an ordering.

PROOF. We already saw that n can be written as a product of primes. (See Proposition 2.5.) So it remains to show the uniqueness part (up to an ordering).

Let $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_m$ be primes such that

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m. \tag{5.1}$$

We want to show that $k = m$ and there is a reordering of $q_1, q_2, \ldots, q_m$ such that $p_i = q_i$ for some $1 \leqslant i \leqslant k = m$. From Equation (5.1), we see

$$p_1 \mid q_1 q_2 \cdots q_m,$$

while p_1 is prime. By Corollary 4.9, there is some $1 \leqslant j \leqslant m$ for which $p_1 \mid q_j$. Both p_1 and q_j are prime, therefore $p_1 = q_j$.

Relabeling and reordering if necessary, we can assume $j = 1$, i.e., $p_1 = q_1$. Dividing Equation (5.1) by $p_1 = q_1$, we obtain

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m.$$

The same argument about $p_1 = q_1$ applies to $p_2 = q_2$, using a reordering (if necessary) of $p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m$.

We can keep this procedure for $p_3, p_4, \ldots, p_k$ and conclude that there is a relabeling of $q_1, q_2, \ldots, q_k$ such that $p_i = q_i$ for all $1 \leqslant i \leqslant k$.

If $m > k$, we divide Equation (5.1) by $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_k$ to get

$$1 = q_{k+1} q_{k+2} \cdots q_m.$$

So we must have $m \leqslant k$. Combining $k \geqslant m$, we have $m = k$. □

A useful reformulation of Theorem 5.1:

THEOREM 5.2 (Prime factorization). *Any integer $n \geqslant 2$ can be written as*

$$n = \prod_{i=1}^{k} p_i^{e_i},$$

where p_i's are distinct primes and e_i's are integers $e_i \geqslant 1$ for $1 \leqslant i \leqslant k$, $k \in \mathbb{Z}$ with $k > 0$. This expression is ***unique*** *up to an ordering. $n = \prod_{i=1}^{k} p_i^{e_i}$ is called* ***prime factorization****.*

PROPOSITION 5.3. *Let $a \geqslant 2$ be an integer and let*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

be the prime factorization of a with p_1, p_2, $\ldots$, p_k distinct primes and $e_i \geqslant 1$ integers for $1 \leqslant i \leqslant k$, $k \in \mathbb{Z}$ with $k > 0$. The positive divisors of a are precisely the elements

$$p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k},$$

where $0 \leqslant d_i \leqslant e_i$ *for each* $1 \leqslant i \leqslant k$*. And these divisors* $p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ *are all distinct.*

Proof. If $b = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ with $0 \leqslant d_i \leqslant e_i$ for each $1 \leqslant i \leqslant k$, $k \in \mathbb{Z}$ with $k > 0$, then $e_i - d_i \geqslant 0$ for each $1 \leqslant i \leqslant k$, we know

$$c = p_1^{e_1-d_1} p_2^{e_2-d_2} \cdots p_2^{e_2-d_2} \in \mathbb{Z}.$$

Also $bc = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ implies $b \mid a$.

Now assume b is a positive divisor of a.

- If $b = 1$, then $b = 1 = p_1^0 p_2^0 \cdots p_k^0$, i.e., $d_1 = d_2 = \cdots = d_k = 0$;
- If $b = a$, then $b = a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, i.e., $d_1 = e_1, d_2 = e_2, \ldots, d_k = e_k$.

Now we assume $b \neq 1, a$. Write $a = bc$. Since $b > 1$ and $b < a$, $1 < c < a$. Apply fundamental theorem of arithmetic (Theorem 5.1) to both b and c. There are primes $q_1, q_2, \ldots, q_m$ and $q_{m+1}, q_{m+2}, \ldots, q_n$ where $m, n \in \mathbb{Z}$, $m > n > 0$, such that

$$\begin{aligned} b &= q_1 q_2 \cdots q_m, \\ c &= q_{m+1} q_{m+2} \cdots q_n. \end{aligned}$$

Then

$$\begin{gathered} a = bc \implies \\ p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1 q_2 \cdots q_m \cdot q_{m+1} q_{m+2} \cdots q_n. \end{gathered}$$

The uniqueness of the prime factorization of a guarantees that each q_j, $j \in \mathbb{Z}$, $1 \leqslant j \leqslant n$, equals some p_i. Moreover, this q_j appears exactly e_i times in

$$q_1 q_2 \cdots q_m \cdot q_{m+1} q_{m+2} \cdots q_n.$$

In particular, for each $1 \leqslant j \leqslant m$, $q_j = p_i$ for some $1 \leqslant i \leqslant k$ and p_i appears at most e_i times in $q_1 q_2 \cdots q_m$. Thus $b = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ with $0 \leqslant d_i \leqslant e_i$ for $1 \leqslant i \leqslant k$. □

Definition 5.4. Let a, b be positive integers. The **least common multiple** of a and b, written as $\operatorname{lcm}(a, b)$, is the smallest positive integer m such that $a \mid m$, $b \mid m$.

Proposition 5.5. *Let* $a, b \in \mathbb{Z}$ *with* $a, b \geqslant 1$*. Let* $p_1, p_2, \ldots, p_k$ *be primes such that*

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \\ b &= p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \end{aligned}$$

with $e_i, f_i \in \mathbb{Z}$*,* $e_i, f_i \geqslant 0$ *for* $1 \leqslant i \leqslant k$*,* k *a positive integer. Then we have*

$$\begin{aligned} \gcd(a, b) &= p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_k^{\min\{e_k, f_k\}}, \\ \operatorname{lcm}(a, b) &= p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_k^{\max\{e_k, f_k\}}. \end{aligned}$$

Sketch of Proof. Left to class as an exercise. Double check [**Str01**, §1.5] for details. ■

Exercise.

5.1. Let $n, k \in \mathbb{Z}$, $n \geqslant k > 0$. Consider k integers

$$1 \leqslant a_1 < a_2 < \cdots < a_k \leqslant n.$$

If any two a_i, a_j, $i \neq j$, $1 \leqslant i, j \leqslant k$, $i, j \in \mathbb{Z}$, satisfy $\operatorname{lcm}(a_i, a_j) > n$, then

$$\sum_{i=1}^{k} \frac{1}{a_i} < \frac{3}{2}.$$

5.2. Let $n, k \in \mathbb{Z}$, $n \geqslant k > 0$. Consider k integers

$$1 \leqslant a_1 < a_2 < \cdots < a_k \leqslant n.$$

If any a_i, $1 \leqslant i \leqslant k$, $i \in \mathbb{Z}$, satisfies

$$a_i \nmid \prod_{\substack{1 \leqslant j \leqslant k \\ i \neq j}} a_j,$$

then $k \leqslant \pi(n)$.

LECTURE 6

Day Six

— 30.01.2017

Recall Proposition 5.5 of last lecture,

Proposition 5.5. *Let $a, b \in \mathbb{Z}$ with $a, b \geqslant 1$. Let $p_1, p_2, \ldots, p_k$ be primes such that*

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

with $e_i, f_i \in \mathbb{Z}$, $e_i, f_i \geqslant 0$ for $1 \leqslant i \leqslant k$, k a positive integer. Then we have

$$\gcd(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_k^{\min\{e_k, f_k\}},$$
$$\operatorname{lcm}(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_k^{\max\{e_k, f_k\}}.$$

Sketch of Proof. If $a = 1$ (or similarly consider $b = 1$) then

$$\gcd(a, b) = 1 = \gcd(1, b),$$
$$\operatorname{lcm}(a, b) = b = \operatorname{lcm}(1, b).$$

Checking the right hand sides of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ respectively in the proposition is straightforward.

Now assume $a, b > 1$, we saw last time (in the proof of Proposition 5.3) that

$$c \mid a \text{ and } c \mid b \iff c = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$$

with $s_i \leqslant e_i$ and $s_i \leqslant f_i$ for $1 \leqslant i \leqslant k$, $s_i \in \mathbb{Z}, s_i \geqslant 0$. This happens if and only if $s_i \leqslant \min\{e_i, f_i\}$ for $1 \leqslant i \leqslant k$. Thus when $s_i = \min\{e_i, f_i\}$ for $1 \leqslant i \leqslant k$ occurs, we have the greatest common divisor of a and b.

The same idea can be used in the case of proving the least common multiple. ■

Corollary 6.1. *For $a, b \in \mathbb{Z}$ with $a, b > 0$, we have*

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$

Proof. (*Hint*: Use the fact that for two real numbers x, y, we have $\min\{x, y\} + \max\{x, y\} = x + y$.) Take $p_1, p_2, \ldots, p_k$ distinct primes such that

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

with $e_i, f_i \in \mathbb{Z}$, $e_i, f_i \geqslant 0$ for $1 \leqslant i \leqslant k$, k a positive integer. Note that for two real numbers x, y,

$$\min\{x, y\} + \max\{x, y\} = x + y.$$

Proposition 5.5 implies

$$\begin{aligned}\gcd(a, b) \operatorname{lcm}(a, b) &= p_1^{\min\{e_1+f_1\}+\max\{e_1+f_1\}} p_2^{\min\{e_2+f_2\}+\max\{e_2+f_2\}} \cdots \\ &\quad p_k^{\min\{e_k+f_k\}+\max\{e_k+f_k\}} \\ &= p_1^{e_1+f_1} p_2^{e_2+f_2} \cdots p_k^{e_k+f_k} \\ &= ab.\end{aligned}$$

We completed the proof. □

Proposition 5.5 gives a conceptual description of the gcd, but it is not very useful in computing. (Since integer factorization is hard.)

One practical way[1] to compute $\gcd(a,b)$ is the **Euclidean algorithm**.

LEMMA 6.2. *Let $a, b \in \mathbb{Z}$, $b \neq 0$. Write $a = bq + r$ with $q, r \in \mathbb{Z}$. Then*

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

PROOF. Left as an exercise.[2] □

Euclidean algorithm: Let $a, b \in \mathbb{Z}$ with $a \geqslant b > 0$.

- Write $a = q_1 b + r_1$ with $q_1, r_1 \in \mathbb{Z}$ and $0 \leqslant r_1 < b$. If $r_1 = 0$, stop;
- If $r_1 \neq 0$, write $b = q_2 r_1 + r_2$ with $q_2, r_2 \in \mathbb{Z}$ and $0 \leqslant r_2 < r_1$. If $r_2 = 0$, stop;
- If $r_2 \neq 0$, write $r_1 = q_3 r_2 + r_3$ with $q_3, r_3 \in \mathbb{Z}$ and $0 \leqslant r_3 < r_2, \ldots$;
- Continue writing $r_{n-1} = q_{n+1} r_n + r_{n+1}$ with $q_{n+1}, r_{n+1} \in \mathbb{Z}$ and $0 \leqslant r_{n+1} < r_n$ until $r_{n+1} = 0$.

THEOREM 6.3. *For $a, b \in \mathbb{Z}$ with $a \geqslant b > 0$, the Euclidean algorithm terminates in finite time. There exists $n \geqslant 1$ such that $r_{n+1} = 0$. Moreover, if $r_{n+1} = 0$ and $r_n \neq 0$, then $\gcd(a,b) = r_n$.*

PROOF. Assume otherwise, if Euclidean algorithm does not terminate in finite time, then

$$b > r_1 > r_2 > \cdots > r_n > \cdots$$

is a strictly decreasing infinite sequence of positive integers. Contradiction.

Therefore there exists $n \geqslant 1$ such that $r_{n+1} = 0$ and $r_n \neq 0$.

Repeatedly apply Lemma 6.2, we have

$$\begin{aligned}\gcd(a,b) &= \gcd(b, r_1)\\ &= \gcd(r_1, r_2)\\ &= \cdots\\ &= \gcd(r_n, r_{n+1})\\ &= \gcd(r_n, 0) && \text{(by } r_{n+1} = 0\text{)}\\ &= r_n > 0.\end{aligned}$$

Hence we completed the proof. □

EXAMPLE 6.4. Compute $\gcd(308, 119)$.

SOLUTION. We can write

$$\begin{aligned}308 &= 2 \times 119 + 70\\ 119 &= 1 \times 70 + 49\\ 70 &= 1 \times 49 + 21\\ 49 &= 2 \times 21 + \underline{7} && \leftarrow \text{last nonzero remainder}\\ 21 &= 3 \times 7 + 0\end{aligned}$$

By Theorem 6.3, we have $\gcd(308, 119) = 7$. □

Recall by Proposition 4.7, there are integers $x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = ax + by.$$

[1] Other (faster, as used in Magma) ways include Accelerated GCD (See [**Web95**]) and Lehmer extended GCD (See [**Knu97**], pp. 345 – 348.)

[2] Hint: Show the set {common divisors of a, b} = {common divisors of b, r}.

We can use Euclidean algorithm to get such x, y by back substitution.

$$\begin{aligned}\gcd(a,b) &= r_n\\ &= r_{n-2} - q_n r_{n-1}.\end{aligned}$$

Plug this into

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2},$$

then continue with

$$r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$$

etc., until we reach the first of this series of equations $a = q_1 b + r_1$. The we have a linear combination in terms of a and b.

Example 6.5. Follow up Example 6.4, write 7 as a linear combination of 308 and 119.

Solution. We know from Example 6.4 that $7 = \gcd(308, 119)$. By back substitution,

$$\begin{aligned}7 &= 49 - 2 \times 21\\ &= 49 - 2 \times (70 - 1 \times 49)\\ &= 49 \times 3 - 2 \times 70\\ &= (119 - 1 \times 70) \times 3 - 2 \times 70\\ &= 119 \times 3 - 70 \times 5\\ &= 119 \times 3 - (308 - 2 \times 119) \times 5\\ &= 308 \times (-5) + 119 \times 13.\end{aligned}$$

□

Exercise.

6.1. Show that x^3 and x^3+x+1 are coprime. (*Hint*: Note that $\gcd(x^3, x^3+x+1) = \gcd(x^3, x+1)$.)

6.2. Let $n \in \mathbb{Z}$, $n > 0$. Show there exists a unique pair $k, \ell \in \mathbb{Z}$ with $0 \leqslant \ell < k$ such that

$$n = \frac{k(k-1)}{2} + \ell.$$

LECTURE 7

Day Seven

— 01.02.2017

Recall Euclid algorithm from last lecture: the algorithm allows us to compute $\gcd(a, b)$, $a, b \in \mathbb{Z}$ and find $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. Hence it is natural to ask

Question: Given $a, b, c \in \mathbb{Z}$ with $a, b > 0$. Consider the equation

$$ax + by = c.$$

When can we solve it for $x, y \in \mathbb{Z}$? If this is the case, can we find all solutions?

This is an example of a linear Diophantine equation (in two variables).

Proposition 7.1. *Let $a, b, c \in \mathbb{Z}$ with a, b not both zero. Then there are $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.*

Proof. Assume there are $x, y \in \mathbb{Z}$ such that

$$ax + by = c.$$

Let $d = \gcd(a, b)$. Since $d \mid a$, $d \mid b$, we have $d \mid (ax + by)$ by Proposition 1.3, i.e., $d = \gcd(a, b) \mid c$.

Now assume $d \mid c$, we want to show there are $x, y \in \mathbb{Z}$ such that

$$ax + by = c.$$

We proved previously (in Proposition 4.7) that there are $m, n \in \mathbb{Z}$ such that

$$am + bn = d.$$

Then there is an integer $e \in \mathbb{Z}$ such that $c = de$ by $d \mid c$, i.e.,

$$a(me) + b(ne) = de = c.$$

So we can take $x = me$ and $y = ne$ as desired. □

Lemma 7.2. *Let $a, b, c \in \mathbb{Z}$, each nonzero. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, we have there exist $m, n \in \mathbb{Z}$ such that

$$1 = am + bn.$$

Multiply both sides by c,

$$c = m(ac) + n(bc).$$

But $a \mid ac$ trivially and $a \mid bc$ by our assumption. So we have $a \mid c$. □

Remark 7.3. Alternatively, we can prove Lemma 7.2 using prime factorization and fundamental theorem of arithmetic. Since $\gcd(a, b) = 1$, a, b share no common divisors. Therefore we must have $a \mid c$ if $a \mid bc$.

It also looks similar to the setting when we proved that if p is prime, $p \mid bc$ and $p \nmid b$ then $p \mid c$. Actually the same proof works here too.

Proposition 7.4. *Let $a, b \in \mathbb{Z}$, not both zero. Let $c \in \mathbb{Z}$. Assume we have $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = c$. Then there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if*

$$x = x_0 + \frac{b}{\gcd(a, b)}k \text{ and } y = y_0 - \frac{a}{\gcd(a, b)}k$$

for $k \in \mathbb{Z}$.

Proof. Let $d = \gcd(a,b)$. Let $a = dr$ and $b = ds$ for some $r, s \in \mathbb{Z}$.

Let $x = x_0 + sk$, $y = y_0 - rk$ for some $k \in \mathbb{Z}$. Then

$$\begin{aligned} ax + by &= a(x_0 + sk) + b(y_0 - rk) \\ &= ax_0 + by_0 + \cancelto{0}{(ask\text{[1]} - brk)} \\ &= c. \end{aligned}$$

Now assume we have $x, y \in \mathbb{Z}$ such that $ax + by = c$. Substituting $ax_0 + by_0 = c$, we have

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0, \\ dr(x - x_0) + ds(y - y_0) &= 0 \implies \\ r(x - x_0) + s(y - y_0) &= 0. \end{aligned}$$

Since $\gcd(r,s) = 1$, $r \mid s(y - y_0) \implies r \mid (y_0 - y)$ by Lemma 7.2. Therefore $y_0 - y = kr$ for some $k \in \mathbb{Z}$. It follows that $y = y_0 - kr$.

Substitute $y = y_0 - rk$ in $ax + by = c$, we have

$$r(x - x_0) = srk.$$

So $x = x_0 + sk$. □

Example 7.5. We saw last time in Example 6.5

$$308 \times (-5) + 119 \times 13 = 7.$$

By Proposition 7.4, the set of integer solutions to

$$308x + 119y = 7$$

is given by

$$\begin{cases} x = -5 + \dfrac{119}{7}k \\ \\ y = 13 - \dfrac{308}{7}k \end{cases}, \text{ for } k \in \mathbb{Z}.$$

<u>Question</u>: How efficient is Euclidean algorithm? For run time, how many steps does it take?

Let $a, b \in \mathbb{Z}$ with $a \geqslant b > 0$. We saw

$$\begin{aligned} a &= q_1 b + r_1, & 0 < r_1 < b \\ b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \; 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0, \quad r_{n+1} = 0. \end{aligned}$$

So it takes $(n+1)$ steps. Can we bound $(n+1)$ in terms of a and b?

A naive analysis: $r_1 < b$ so

$$\begin{aligned} r_1 &\leqslant b - 1, \\ r_2 &\leqslant r_1 - 1 \leqslant b - 2, \\ &\vdots \\ r_n &\leqslant b - n, \\ 0 = r_{n+1} &\leqslant b - (n+1). \end{aligned}$$

Hence $n \leqslant b - 1$. The naive bound $(n+1) \leqslant b$.

[4] Not the word “ask”.

LECTURE 8

Day Eight

— 03.02.2017

Recall from last time, the naive bound of Euclid algorithm is $(n+1) \leqslant b$. We can improve this bound however,

Claim 8.1. The #steps of Euclidean algorithm satisfies $(n+1) \leqslant 2\log_2 b$.

Proof. We can analyze Euclidean algorithm two steps at a time.

First, we look at the two equations

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2. \end{aligned}$$

(i) If $r_1 \leqslant \frac{b}{2}$, then $r_2 < r_1 \leqslant \frac{b}{2}$.

(ii) If $\frac{b}{2} < r_1 < b$, then $r_2 = b - q_1 r_1 < \frac{b}{2}$ by $q_1 \geqslant 1$, a, b positive integers.

In either case, $r_2 < \frac{b}{2}$. Same arguments show that

$$r_{k+1} < \frac{r_{k-1}}{2}$$

for any $k \in \mathbb{Z}$, $k > 0$. Therefore, $r_2 < \frac{b}{2}$, $r_4 < \frac{b}{4}$, $r_6 < \frac{b}{8}$, $\dots$, i.e., we have

$$r_{2k} < \frac{b}{2^k}$$

for any $k \in \mathbb{Z}$, $k > 0$. If $\frac{b}{2^k} = 1$ then $r_{2k} < \frac{b}{2^k} = 1 \implies r_{2k} = 0$.

Hence $(n+1) \leqslant 2k = 2\log_2 b$. □

Remark 8.2. Up to constants, $(n+1) \leqslant 2\log_2 b$ is the best possible.

Example 8.3. Consider the Fibonacci sequence, defined as follows,

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1, \dots, F_{n+1} = F_n + F_{n-1} \text{ for all } n \geqslant 2.$$

Run Euclidean algorithm to compute $\gcd(F_{n+1}, F_n)$.

$$\begin{aligned} F_{n+1} &= 1 \cdot F_n + F_{n-1}, \\ &\vdots \\ F_4 &= 1 \cdot F_3 + F_2, \\ F_3 &= 1 \cdot F_2 + F_1 = 2 \cdot 1 + 0. \end{aligned}$$

We can see the run time in this computation is #steps $= n - 1$. One can show[1] there are constants b_1, c_1 such that for each n

$$c_1 b_1^n \leqslant F_n \leqslant c_1 b_1^n + 1.$$

Hence $n \geqslant b_2 \log_2 F_n + c_2$ for some b_2, c_2. Therefore the #steps it takes to compute $\gcd(F_{n+1}, F_n)$ satisfies $n - 1$ steps $\geqslant b_2 \log_2 F_n + c_2 - 1$.

But maybe there is a better algorithm?

[1] No proof was given in the lecture. It is known $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$.

Conjecture 8.4. *For any algorithm computing* gcd *using only "remainder function", i.e., given a and b, output r such that $a = bq + r$ with $0 \leqslant r < b$, there is a positive constant c such that*

$$\#\textit{steps to compute } \gcd(a,b) \ \geqslant c \log_2 a$$

for infinitely many pairs a and b with $a \geqslant b > 0$.

Theorem 8.5 (Moschovakis–van den Dries). *For any algorithm using only $+$, $-$, "quotient function and remainder functions", i.e., given a, b output r such that $a = bq + r$ with $0 \leqslant r < b$, then there are infinitely many $a \geqslant b > 0$ such that*

$$\#\textit{steps to compute } \gcd(a,b) \ \geqslant \frac{1}{6} \log_2 \log_2 a.$$

Remark 8.6. For the proof, the class is referred to [**MvdD04**]. This holds whenever $a^2 - 2b^2 = 1$ and $b > 2$. The right hand side of the inequality is independent of b meaning there are infinitely many such pairs.

Congruences

Definition 8.7. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say a **is congruent to** b **modulo** n, written as $a \equiv b \bmod n$, if $n \mid (a - b)$; if a is not congruent to b modulo n, we write $a \not\equiv b \bmod n$.

Example 8.8. $212 \equiv 0 \bmod 2$. $212 \equiv 2 \bmod 5$. $212 \not\equiv 13 \bmod 5$.

Proposition 8.9. *Let $n > 0$ be a positive integer. Congruence modulo n is an equivalence relation on $\mathbb{Z}$, i.e., congruences modulo n satisfies the following:*

(1) It is reflexive. For all $a \in \mathbb{Z}$, $a \equiv a \bmod n$;
(2) It is symmetric. For all $a, b \in \mathbb{Z}$, if $a \equiv b \bmod n$ then $b \equiv a \bmod n$;
(3) It is transitive. For any $a, b, c \in \mathbb{Z}$, if $a \equiv b \bmod n$, $b \equiv c \bmod n$, then $a \equiv c \bmod n$.

Proof. We need to check the above three conditions.

(i) Reflexivity. $a - a = 0$ and $n \mid 0$.
(ii) Symmetry. $a \equiv b \bmod n$ implies $n \mid (a - b)$. We can write $a - b = cn$ for some $c \in \mathbb{Z}$. Thus $b - a = (-c)n$, i.e., $n \mid (b - a)$.
(iii) Transitivity. By $a \equiv b \bmod n$, $b \equiv c \bmod n$ we can write $a - b = xn$, $b - c = yn$ for some $x, y \in \mathbb{Z}$. Then $a - c = (x + y)n$, i.e., $n \mid (a - c)$.

□

Exercise.

8.1. Compared with Claim 8.1, show the #steps of Euclidean algorithm to compute $\gcd(a, b)$, $a, b \in \mathbb{Z}$, $a > b > 0$, also satisfies $(n + 1) \leqslant 5\ell$, where $\ell =$ #digits of b.

8.2. Let $a, n \in \mathbb{Z}$ with $a, n > 1$. $b = a^n$ is called a perfect power. Let p be a prime. Show that $2^p + 3^p$ is not a perfect power.

8.3. Let $n \in \mathbb{Z}$. Show that
(a) if $n > 1$, there does not exist an odd prime p and a positive integer m such that $p^n + 1 = 2^m$;
(b) if $n > 2$, there does not exist an odd prime p and a positive integer m such that $p^n - 1 = 2^m$.

8.4. Given any integer $n \in \mathbb{Z}$, it must satisfy one of these congruences: $n \equiv 0 \bmod 2$, $n \equiv 0 \bmod 3$, $n \equiv 1 \bmod 4$, $n \equiv 5 \bmod 6$, or $n \equiv 7 \bmod 12$. (*Hint*: Consider congruence class of any odd integer modulo 12.)

LECTURE 9

Day Nine

— 06.02.2017

Recall from last time, let $a, b, n \in \mathbb{Z}$ with $n > 0$, we say a is a congruent to b modulo n if $n \mid (a-b)$.

DEFINITION 9.1. Let $n \in \mathbb{Z}$, $n > 0$ and let $a \in \mathbb{Z}$. The set of all integers congruent to a modulo n is called a **congruence class modulo** n. And we denote this class by $[a]$.

EXAMPLE 9.2. What are the congruence classes modulo 2?

$$\begin{aligned}\{\text{even integers}\} &= [0] = [2] = \cdots,\\ \{\text{odd integers}\} &= [1] = [-1] = \cdots.\end{aligned}$$

Say $n \in \mathbb{Z}$, $n > 0$ and $a, b \in \mathbb{Z}$, when is $[a] = [b]$?

CLAIM 9.3. $[a] = [b]$ if and only if $a \equiv b \bmod n$.

PROOF. ($\Rightarrow$) If $[a] = [b]$, then $b \in [a]$. So $a \equiv b \bmod n$.
($\Leftarrow$) If $a \equiv b \bmod n$, for $c \in [a]$, it follows that by transitivity, $c \equiv a \bmod n$ and $a \equiv b \bmod n$ imply $c \equiv b \bmod n$. So $[a] \subseteq [b]$. Similarly, we have $[b] \subseteq [a]$. □

Consequently,

$$\begin{aligned}[a] = [b] &\iff a \equiv b \bmod n\\ &\iff b \in [a].\end{aligned}$$

Then if $a \not\equiv b \bmod n$, what can be said about $[a], [b]$?

CLAIM 9.4. If $[a] \neq [b]$, then $[a] \cap [b] = \varnothing$.

PROOF. If $[a] \cap [b] \neq \varnothing$, then there is a $c \in \mathbb{Z}$ such that $c \in [a]$ and $c \in [b]$, meaning $c \equiv a \bmod n$ and$c \equiv b \bmod n$. Hence $[a] = [c] = [b]$ by Claim 9.3, a contradiction. □

Aside, a contrapositive of a statement "$p \implies q$" is "not $q \implies$ not p."

EXAMPLE 9.5. What do the congruence classes modulo 3 look like?
They are $[0], [1], [2]$. Generally, fix a,

$$\begin{aligned}[a] &= \{b : b \in \mathbb{Z}, b \equiv a \bmod 3\}\\ &= \{a + 3k : k \in \mathbb{Z}\}.\end{aligned}$$

DEFINITION 9.6. Let $n \in \mathbb{Z}$, $n > 0$, a set $\mathcal{S}$ of integers is called a **complete residue system modulo** n, if every integer is congruent to *precisely* one element of $\mathcal{S}$.

PROPOSITION 9.7. *Let $n \in \mathbb{Z}$, $n > 0$. Then $\{0, 1, \ldots, n-1\}$ is a* ***complete*** *residue system modulo n.*

PROOF. Let $a \in \mathbb{Z}$. We first show a is congruent to some element in $\{0, 1, \ldots, n-1\}$. By division algorithm, there are unique $q, r \in \mathbb{Z}$ such that $a = qn + r$ with $0 \leqslant r < n$. So $n \mid (a - r)$ and $r \in \{0, 1, \ldots, n-1\}$. We then have $a \equiv r \bmod n$.
Now assume $r' \in \{0, 1, \ldots, n-1\}$ satisfies $a \equiv r' \bmod n$. Then $a = q'n + r'$ for some $q' \in \mathbb{Z}$. But $0 \leqslant r' < n$, the uniqueness of q and r in the division algorithm implies $r' = r$. □

Consequently, another way to think of congruences is that $a \equiv b \bmod n \iff$ dividing a and b by n, à la division algorithm, gives the same remainder.

Proposition 9.8. *Let $a, b, c, d \in \mathbb{Z}$ and let $n \in \mathbb{Z}$, $n > 0$. Assume $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then*

(1) $a + c \equiv b + d \bmod n$;
(2) $ac \equiv bd \bmod n$.

Proof. We have to prove two statements.

(i) $a \equiv b \bmod n$ implies $n \mid (a - b)$, i.e., $a = b + k_1 n$ for some $k_1 \in \mathbb{Z}$. Similarly, $c = d + k_2 n$ for some $k_2 \in \mathbb{Z}$. Then we have

$$\begin{aligned}(b + d) - (a + c) &= (b + d) - ((b + k_1 n) + (d + k_2 n)) \\ &= -(k_1 + k_2)n.\end{aligned}$$

Therefore $n \mid (b + d) - (a + c) \bmod n$, i.e., $a + c \equiv b + d \bmod n$.

(ii) Follow (i), we can check

$$\begin{aligned}ac - bd &= (b + k_1 n)(d + k_2 n) - bd \\ &= (k_1 d + k_2 b + n k_1 k_2)n.\end{aligned}$$

Therefore $n \mid (ac - bd)$, i.e., $ac \equiv bd \bmod n$.

We completed the proof. □

Consequently, we can define "addition" and "multiplication" on residue classes modulo n by

$$\begin{aligned}[][a] + [c] &= [a + c], \\ [a][c] &= [ac].\end{aligned}$$

They make sense only when Proposition 9.8 holds.

Exercise.

9.1. Let p be a prime. Show that

(a) $\displaystyle\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \bmod p$;

(b) if $p^s \;\Big|\; \left\lfloor \frac{n}{p} \right\rfloor$ for some $s \in \mathbb{Z}$, $s > 0$, then $p^s \;\Big|\; \binom{n}{p}$.

9.2. Let $n \in \mathbb{Z}$. Show that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is also an integer.

9.3. Let p be an odd prime with $p > 3$. Show for any $a, b \in \mathbb{Z}$, $ab^p - ba^a \equiv 0 \bmod 6p$. (*Hint*: Note that $6 \mid b(b^2 - 1)$.)

LECTURE 10

Day Ten

— 08.02.2017

Recall Proposition 9.8 from last time,

PROPOSITION 9.8. *Let $a, b, c, d \in \mathbb{Z}$ and let $n \in \mathbb{Z}$, $n > 0$. Assume $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then*

(1) $a + c \equiv b + d \bmod n$;
(2) $ac \equiv bd \bmod n$.

Thus *addition* and *multiplication* modulo n depends only on congruence classes. Addition and multiplication on congruence classes are well defined by

$$\begin{aligned}[a] + [c] &= [a + c],\\ [a][c] &= [ac].\end{aligned}$$

EXAMPLE 10.1. $2 + 5 \equiv 7 \equiv 1 \bmod 6$. $8 + 23 \equiv 31 \equiv 1 \bmod 6$.

EXAMPLE 10.2. Working with modulus 6, we have $[2] = [8]$ and $[5] = [23]$. Then $[2]+[5] = [8]+[23]$ since $[7] = [1] = [31]$.

EXAMPLE 10.3. Working with modulus 2, we have the familiar assertion in grade school,

$$\begin{aligned}\text{even} + \text{even} &= \text{even},\\ \text{even} + \text{odd} &= \text{odd},\\ \text{odd} + \text{odd} &= \text{even}.\end{aligned}$$

Similarly with multiplication,

$$\begin{aligned}\text{even} \times \text{even} &= \text{even},\\ \text{even} \times \text{odd} &= \text{even},\\ \text{odd} \times \text{odd} &= \text{odd}.\end{aligned}$$

Another (down-to-earth) way to think about this: from last lecture, we saw in Proposition 9.7 that $\{0, 1, \dots, n-1\}$ is a complete residue system modulo n. So $[0], [1], \dots, [n-1]$ are distinct congruence classes. Then if $0 \leqslant a, c \leqslant n-1$, $[a]+[c] = [r]$ with $a+c = qn+r$ and $0 \leqslant r < n$ by division algorithm.

Similar argument applies to $[a][c] = [r']$ with $ac = q'n + r'$ and $0 \leqslant r' < n$.

NOTATION 10.4. The set of congruence classes with the above operations of addition and multiplication is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

EXAMPLE 10.5. Consider addition of elements in $\mathbb{Z}_3$,

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

.

Consider multiplication of elements in $\mathbb{Z}_3$,

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Example 10.6. Consider addition of elements in $\mathbb{Z}_4$,

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Consider multiplication of elements in $\mathbb{Z}_4$,

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Note that the multiplication of two nonzero elements $[2], [2]$ gives zero in the multiplication table.

Remark 10.7. Usual arithmetic rules hold modulo n except for $[a], [b] \neq 0$, we could still have $[a][b] = 0$ (or $[a][b] = 0$ does not necessarily imply $[a] = 0$ or $[b] = 0$.) Such nonzero a, b that $ab = 0$ are called **zero divisors** (in a **ring**). Consequently, cancellation modulo n is not trivial. In the above Example 10.6, $2 \times 2 \equiv 0 \bmod 4$ but $2 \not\equiv 0 \bmod 4$.

Proposition 10.8. *Let $a, b, c, n \in \mathbb{Z}$, $n > 0$. Then $ca \equiv cb \bmod n$ if and only if $a \equiv b \bmod \frac{n}{\gcd(c,n)}$.*

Proof. $(\Rightarrow)$ Assume $ca \equiv cb \bmod n$. Then $n \mid (ca - cb)$. Let $d = \gcd(c, n)$, we have $\frac{n}{d} \mid \frac{c}{d}(a - b)$. But $\frac{n}{d}, \frac{c}{d}$ are coprime, by Lemma 7.2, we have $\frac{n}{d} \mid (a - b)$, i.e., $a \equiv b \bmod \frac{n}{d}$.

$(\Leftarrow)$ If $a \equiv b \bmod n$, then $a - b = e\left(\frac{n}{d}\right)$ for some $e \in \mathbb{Z}$. It further implies $d(a - b) = en$. We also know that $c = fd$ for some $f \in \mathbb{Z}$. So $(fd)(a - b) = c(a - b) = (fe)n$, i.e., $ca \equiv cb \bmod n$. □

For $a, b, n \in \mathbb{Z}$, $n > 0$, an equation $ax \equiv b \bmod n$ is called a **linear congruence equation modulo** n.

Question: When can we find a solution $x \in \mathbb{Z}$ to this equation?

If a solution exists, it means $\exists\, x \in \mathbb{Z}$ such that $n \mid (ax - b)$, i.e., $ax - b = ny$ for some $y \in \mathbb{Z}$. Thus if a solution exists it implies $\exists\, x, y \in \mathbb{Z}$ such that $ax - ny = b$ (Diophantine equation in two variables). Therefore, $ax \equiv b \bmod n$ has an integer solution if and only if b is a linear combination of a and n. Further, it has a solution if and only if $\gcd(a, n) \mid b$.

Example 10.9. $10x \equiv 5 \bmod 12$ has no solutions since $\gcd(10, 12) = 2 \nmid 5$. $10x \equiv 8 \bmod 12$ has solutions however, since $\gcd(10, 12) = 2 \mid 8$.

We saw in Proposition 7.4 that if $x_0, y_0 \in \mathbb{Z}$ satisfy $ax_0 + ny_0 = b$, then the complete set of solutions to $ax + ny = b$ is given by

$$\begin{cases} x = x_0 + \dfrac{n}{\gcd(a,n)}k \\[2ex] y = y_0 - \dfrac{a}{\gcd(a,n)}k \end{cases}, \text{ for } k \in \mathbb{Z}\,.$$

The set of solutions to $ax \equiv b \bmod n$

$$x = x_0 + \frac{n}{\gcd(a,n)}k, \text{ for } k \in \mathbb{Z},$$

when modulo n, these x's repeat and there are $\gcd(a,n)$ many distinct solutions modulo n. And they are given by

$$x_0,\, x_0 + 1\left(\frac{n}{a}\right),\, \ldots,\, x_0 + (d-1)\left(\frac{n}{a}\right),$$

where $d = \gcd(a,n)$. So we have the following theorem.

THEOREM 10.10. *The linear congruence* $ax \equiv b \bmod n$ *has a solution if and only if* $\gcd(a,n) \mid b$. *If this is the case, it has* $\gcd(a,n)$ *many distinct solutions modulo* n.

COROLLARY 10.11. *If* $\gcd(a,n) = 1$, *then* $ax \equiv b \bmod n$ *has a* ***unique*** *solution modulo* n.

COROLLARY 10.12. $ax \equiv 1 \bmod n$ *has a solution if and only if* $\gcd(a,n) = 1$.

If $ax \equiv 1 \bmod n$ for some $x \in \mathbb{Z}$, we say x is the **multiplicative inverse of** a **modulo** n. If such an inverse of a modulo n exists, written as a^{-1}, it is unique modulo n.

Exercise.

10.1. Let $n \in \mathbb{Z}$. Show $504 \mid n^9 - n^3$.

10.2. Solve $(n-1)! = n^k - 1$ for all $n, k \in \mathbb{Z}$. (*Hint*: There are three solutions: $(n,k) = (2,1)$, $(3,1)$, and $(5,2)$. Show when $n > 5$, there are no integer solutions.)

LECTURE 11

Day Eleven

— 10.02.2017

Recall last time we saw $a \in \mathbb{Z}$ has a multiplicative inverse modulo n, i.e., $ax \equiv 1 \bmod n$ has an integer solution x if and only if $\gcd(a, n) = 1$.

Definition 11.1. The **Euler φ-function**, denoted φ, is given by

$$\varphi(n) = |\{a \in \mathbb{Z} : 1 \leqslant a \leqslant n,\ \gcd(a, n) = 1\}|$$

for any positive integer n.

Example 11.2. Quick examples.

- $\varphi(6) = 2$ with $n = 6$, $a = 1, 5$.
- $\varphi(10) = 4$ with $n = 10$, $a = 1, 3, 7$ and 9.
- $\varphi(15) = 8$ with $n = 15$. Later we will know that $\varphi(15) = \varphi(3)\varphi(5) = (3 - 1) \times (5 - 1)$.
- If p is prime, $\varphi(p) = p - 1$.

For a fixed $n \in \mathbb{Z}$, $n > 0$ and a prime p, either $p \mid n$ or $\gcd(p, n) = 1$.

Theorem 11.3 (Dirichlet). *For any $a, n \in \mathbb{Z}$, $n > 0$ and $\gcd(a, n) = 1$, there are infinitely many primes congruent to a modulo n. Phrased another way, it says there are infinitely many primes in the arithmetic progression,*

$$a,\ a + n,\ \ldots, a + kn,\ \ldots$$

where $k \in \mathbb{Z}$, $k > 0$.

Remark 11.4. Dirichlet's theorem on arithmetic progressions is one of the "biggest" theorems in analytic number theorem. The proof is beyond this course therefore it will not be given in the lecture. A related theorem about primes in arithmetic progression is Green-Tao [**GT08**], which states that the sequence of primes contains arbitrarily long arithmetic progressions.

Example 11.5. There are infinitely many primes of the form $4k + 1$ and $4k + 3$, where $k \in \mathbb{Z}$, $k > 0$.

Recall the prime counting function

$$\pi(x) = |\{p : p \text{ is prime}, p \leqslant x\}|$$

and the prime number theorem which states

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

Let $a, n \in \mathbb{Z}$, $n > 0$. Define

$$\pi(x; n, a) = |\{p \leqslant x : p \text{ is prime}, p \equiv a \bmod n\}|.$$

Theorem 11.6 (Dirichlet's theorem, strong form). *If $\gcd(a, n) = 1$, then*

$$\pi(x; n, a) \sim \frac{1}{\varphi(n)} \frac{x}{\log x}.$$

Remark 11.7. The moral of the strong form of Dirichlet's theorem is that to the first order, primes are evenly distributed among the residue classes modulo n that are coprime with n. Computationally, it seems some residue classes actually have "more" primes, i.e., the second order term of the distribution of primes among the residue classes modulo n is different.

Conjecture 11.8. *Let $a, b, n \in \mathbb{Z}$, $0 < a, b < n$ with $\gcd(a, n) = \gcd(b, n) = 1$. If a is a quadratic residue*[1] *modulo n while b is a quadratic nonresidue modulo n, then $\pi(x; n, b) > \pi(x; n, a)$ more often than not.*

Remark 11.9. $\pi(x; 4, 3) > \pi(x; 4, 1)$ more often than not. The density of such x is greater than 0.99. This phenomenon was first observed by P. Chebyshev in the 1850s. The problem is called **Chebyshev bias** or **prime number race**.

We restate the second half of Example 11.5 as a theorem and prove it below without using Dirichlet's theorem but using an elementary way instead.

Theorem 11.10. *There are infinitely many primes congruent to 3 modulo 4. Equivalently, there are infinitely many primes of the form $4k + 3$, where $k \in \mathbb{Z}$, $k \geqslant 0$.*

Proof. Assume the contrary, there are only finitely many primes of the form $4k+3$, where $k \in \mathbb{Z}$, $k \geqslant 0$. Label them as

$$p_0, p_1, \ldots, p_m \text{ with } p_0 = 3,\ m \in \mathbb{Z},\ m > 0.$$

Consider the number $N = 4p_1p_2 \cdots p_m + 3$. Obviously $N \equiv 3 \bmod 4$.

(i) $2 \nmid N$ since otherwise $2 \mid N - 4p_1p_2 \cdots p_m = 3 \implies 2 \mid 3$, a contradiction.
(ii) Similarly, $p_i \nmid N$ for $1 \leqslant i \leqslant m$. (Otherwise $p_i \mid 3$ for $1 \leqslant i \leqslant m$.)
(iii) Lastly, $3 \nmid N$ since otherwise $3 \mid N - 3 \implies 3 \mid 4p_1p_2 \cdots p_m$. Then $3 \mid p_i$ for some $1 \leqslant i \leqslant m$ by 3 being a prime, a contradiction.

Therefore, N has no divisors d, $d \in \mathbb{Z}$ such that $d \equiv 0, 2 \bmod 4$ (by $2 \nmid N$) or $d \equiv 3 \bmod 4$ (by $N > 1$ has a prime divisor but those primes of the form $4k + 3$ have been ruled out; there are finitely many and none of them divides N.) So the only divisors of N are congruent to 1 modulo 4.

We can write $N = q_1q_2 \cdots q_n$, $q_j \equiv 1 \bmod 4$ for $1 \leqslant j \leqslant n$, $n \in \mathbb{Z}$ and $n > 0$. Then we have

$$\begin{aligned} N &= q_1q_2 \cdots q_n \\ &\equiv 1 \cdot 1 \cdot \cdots \cdot 1 \bmod 4 \\ &\equiv 1 \bmod 4, \end{aligned}$$

a contradiction. □

Back to linear congruence equations, clearly, $x \equiv b \bmod n$ has a unique solution modulo n.

Question: Can we find $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

with $a, b, m, n \in \mathbb{Z}$, $m, n > 0$?

Example 11.11. Solve linear congruences

$$\begin{cases} x \equiv 4 \bmod 7 \\ x \equiv 5 \bmod 9. \end{cases}$$

Solution. We can write $x - 4 = 7\ell$ and $x - 5 = 9q$, where $\ell, q \in \mathbb{Z}$. If we plug the second equation into the first one, then we have $7\ell + 4 = 9q + 5$, i.e., $7\ell \equiv 1 \bmod 9$. We use Euclidean algorithm to solve for ℓ,

$$\begin{aligned} 9 &= 1 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

[1] We will discuss "quadratic residue/nonresidue modulo n" in detail later in the course.

By back substitution,

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3 \times (9 - 7) \\ &= 4 \times 7 - 3 \times 9. \end{aligned}$$

So we can take $\ell = 4$. $x = 4 + 7 \times 4 = 32$. $x = 32$ solves

$$\begin{cases} x \equiv 4 \bmod 7 \\ x \equiv 5 \bmod 9. \end{cases}$$

□

Exercise.

11.1. Let $a, m, n \in \mathbb{Z}$, $m, n > 0$ with $\gcd(a, n) = 1$. Consider arithmetic progression

$$a,\ a + n,\ \ldots, a + kn,\ \ldots$$

where $k \in \mathbb{Z}$, $k > 0$. Show there are infinitely many k's such that $\gcd(a + kn, m) = 1$.

LECTURE 12

Day Twelve

— 13.02.2017

Chinese remainder theorem (CRT)

THEOREM 12.1. *Let $n_1, n_2, \ldots, n_k$ be coprime positive integers, i.e,* $\gcd(n_i, n_j) = 1$ *if $i \neq j$ for $1 \leqslant i, j \leqslant k$ where $k \in \mathbb{Z}$, $k > 0$. Let $b_1, b_2, \ldots, b_k \in \mathbb{Z}$. The system of congruences*

$$\begin{aligned} x &\equiv b_1 \bmod n_1 \\ x &\equiv b_2 \bmod n_2 \\ &\vdots \\ x &\equiv b_k \bmod n_k \end{aligned}$$

has a ***unique*** *solution modulo $(n_1 n_2 \cdots n_k)$.*

PROOF. [1]We induct on $k \geqslant 1$.

To prove the existence of such an x, if $k = 1$, it is clear that

$$x_1 \equiv b_1 \bmod n_1$$

has a unique solution modulo n_1.

Assume the result is true for $k - 1 \geqslant 1$. By our induction hypothesis, there is an $x_0 \in \mathbb{Z}$ such that

$$\begin{aligned} x_0 &\equiv b_1 \bmod n_1 \\ x_0 &\equiv b_2 \bmod n_2 \\ &\vdots \\ x_0 &\equiv b_{k-1} \bmod n_{k-1}, \end{aligned}$$

and it is unique modulo $N = n_1 n_2 \cdots n_{k-1}$. Now consider the system of two congruences

$$x \equiv x_0 \bmod N \tag{12.1}$$

$$x \equiv b_k \bmod n_k. \tag{12.2}$$

Equation (12.2) implies $x - b_k = n_k \ell$ for some $\ell \in \mathbb{Z}$.

Plug $x = b_k + n_k \ell$ into Equation (12.1), we have

$$n_k \ell \equiv x_0 - b_k \bmod \prod_{i=1}^{k-1} n_i. \tag{12.3}$$

Since $\gcd(n_k, n_i) = 1$ for $1 \leqslant i \leqslant k - 1$, it implies $\gcd(n_k, \prod_{i=1}^{k-1} n_i) = 1$. Indeed, if there is a prime p such that $p \mid n_k$ and $p \mid \prod_{i=1}^{k-1} n_i$, then $p \mid n_i$ for some $1 \leqslant i \leqslant k - 1$. Hence $\gcd(n_k, n_i) \neq 1$ for some $1 \leqslant i \leqslant k - 1$.

Since $\gcd(n_k, \prod_{i=1}^{k-1} n_i) = 1$ in Equation (12.3), we can find $\ell \in \mathbb{Z}$ such that

$$n_k \ell \equiv x_0 - b_k \bmod N.$$

[1] This proof is based on the technique used in Example 11.11 then apply induction. The proof is different from [**Str01**, §2.3, Theorem 2.9], which is quite tricky.

Set $x = b_k + n_k \ell$. Clearly $x \equiv b_k \bmod n_k$. And by construction

$$x \equiv x_0 \bmod \prod_{i=1}^{k-1} n_i,$$

therefore by reducing the modulus to its divisor[2],

$$\begin{aligned} x &\equiv x_0 \bmod n_i \\ &\equiv b_i \ \bmod n_i \end{aligned} \tag{12.4}$$

for each $1 \leqslant i \leqslant k-1$. The second congruence in Equation (12.4) is by our induction hypothesis.

To prove the uniqueness of this x, let $y \in \mathbb{Z}$ be another solution such that $y \equiv b_i \bmod n_i$ for each $1 \leqslant i \leqslant k$. Our induction hypothesis (x is unique up to $k-1$ congruences) gives

$$\begin{aligned} y &\equiv x_0 \bmod n_1 n_2 \cdots n_{k-1} \\ &\equiv x \quad \bmod n_1 n_2 \cdots n_{k-1}. \end{aligned}$$

Together with $y \equiv x \bmod n_k$, we have

$$\begin{aligned} n_1 n_2 \cdots n_{k-1} &\mid y - x, \\ n_k &\mid y - x. \end{aligned}$$

Therefore[3] $\operatorname{lcm}(\prod_{i=1}^{k-1} n_i, n_k) \mid y - x$. But $\gcd(\prod_{i=1}^{k-1} n_i, n_k) = 1$, so $\operatorname{lcm}(\prod_{i=1}^{k-1} n_i, n_k) = n_k \prod_{i=1}^{k-1} n_i = \prod_{i=1}^{k} n_i$. Hence $n_1 n_2 \cdots n_k \mid y - x$, i.e., $y \equiv x \bmod n_1 n_2 \cdots n_k$. □

Remark 12.2. In practice, we can solve these congruences inductively by first finding a solution to the first $k-1$ congruences. Then solve the two congruences

$$\begin{aligned} x &\equiv x_0 \bmod n_1 n_2 \cdots n_{k-1} \\ x &\equiv b_k \ \bmod n_k. \end{aligned}$$

Example 12.3. Find a solution to

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 4 \\ x &\equiv 4 \bmod 5. \end{aligned}$$

Solution. The first congruence implies $x = 3k + 1$ for some $k \in \mathbb{Z}$. Plug it into the second congruence, we have

$$\begin{aligned} 1 + 3k &\equiv 2 \bmod 4 \implies \\ 3k &\equiv 1 \bmod 4. \end{aligned}$$

Quick inspection tells us we can take $k = 3$. So $x = 3 \times 3 + 1 = 10$ solves the first two congruences

$$\begin{aligned} x &\equiv 1 \bmod 3 \\ x &\equiv 2 \bmod 4. \end{aligned}$$

By Chinese remainder theorem, the first two congruences are equivalent to $x \equiv 10 \bmod 12$. Hence we reduce the original system of congruences to

$$\begin{aligned} x &\equiv 10 \bmod 12 \\ x &\equiv 4 \quad \bmod 5. \end{aligned}$$

[2] Trick!

[3] Similar to what we have seen for the greatest common divisors $\{d : d = \text{common divisors of } a, b\} = \{\text{multiples of } \gcd(a, b)\}$, we have $\{e : e = \text{common multiples of } a, b\} = \{\text{multiples of } \operatorname{lcm}(a, b)\}$.

Repeat the first step in this example to solve the new system of two congruences. The first congruence in the new system implies $x = 10 + 12\ell$ for some $\ell \in \mathbb{Z}$. Plug it into the second equation $x \equiv 4 \bmod 5$, we have

$$\begin{aligned} 10 + 12\ell &\equiv 4 \bmod 5 \implies \\ 0 + 2\ell &\equiv 4 \bmod 5. \end{aligned}$$

So we can take $\ell = 2$. Thus $x = 10 + 2 \times 2 = 34$ solves the original three congruences. It is unique modulo $3 \times 4 \times 5 = 60$. □

Notice that in the previous example we used/saw

$$3^2 \equiv 1 \bmod 4.$$

Actually, $\gcd(3, 4) = 1$ and $\varphi(4) = 2$ in this case.

Recall the Euler φ-function,

$$\varphi(n) = |\{a \in \mathbb{Z} : 1 \leqslant a \leqslant n, \gcd(a, n) = 1\}|.$$

Theorem 12.4 (Euler's theorem). *Let $a, n \in \mathbb{Z}$, $n > 0$ and $\gcd(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Proof. Euler's theorem will be proved in Lecture 13. □

Corollary 12.5 (Fermat's little theorem). *For any prime p and $a \in \mathbb{Z}$ with $p \nmid a$, we have*

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

Proof. Assuming Euler's theorem, if $p \nmid a$, then $\gcd(a, n) = 1$. It follows from Euler's theorem that $a^{p-1} \equiv 1 \bmod p$ since $\varphi(p) = p - 1$. □

Corollary 12.6 (of Fermat's little theorem). *For any prime p and any $a \in \mathbb{Z}$, we have*

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

Proof. We consider two cases.

(i) If $p \nmid a$, we can apply Fermat's little theorem. Then $a^{p-1} \equiv 1 \bmod p \implies a^{p-1} \cdot a \equiv 1 \cdot a \bmod p$, i.e., $a^p \equiv a \bmod p$.

(ii) If $p \mid a$, then $p \mid a^p$. Therefore

$$\begin{aligned} a^p &\equiv 0 \bmod p \\ &\equiv a \bmod p. \end{aligned}$$

We completed the proof. □

Example 12.7. Find the smallest positive integer in the congruence class of $3^{537} \bmod 11$.

Solution. By Fermat's little theorem,

$$3^{10} \equiv 1 \bmod 11.$$

Therefore

$$\begin{aligned} 3^{537} &= (3^{10})^{53} \times 3^7 \\ &\equiv 1^{53} \times 3^7 \quad \bmod 11 \\ &\equiv (3^2)^3 \times 3 \quad \bmod 11 \\ &\equiv (-2)^3 \times 3 \bmod 11 \\ &\equiv -24 \bmod 11 \\ &\equiv 9 \qquad \bmod 11. \end{aligned}$$

Note that even with 3^7, we still want to reduce it to a smaller number that is manageable. □

Exercise.

12.1. Let (a_n) be a sequence in $\mathbb{Z}_{>0}$ with $a_{n+1} = 2a_n + 1$ for $n = 1, 2, \ldots$ Show that it cannot be the case that all a_n's are prime. (*Hint*: Let p be an odd prime. Then $p \mid 2^{p-1}p + 2^{p-1} - 1$.)

12.2. Find the smallest positive integer n such that $\frac{1}{2}n$ is a square; $\frac{1}{3}n$ is a cube; and $\frac{1}{5}n$ is a fifth power.

LECTURE 13

Day Thirteen

— 15.02.2017

Recall Euler's theorem from last time,

THEOREM 12.4 (Euler's theorem). *Let $a, n \in \mathbb{Z}$, $n > 0$ and $\gcd(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Recall the notation $\varphi(n)$, which is the Euler φ-function counting all the positive integers up to n that are coprime with n.

PROOF (of Euler's theorem). Let $r_1, r_2, \ldots, r_{\varphi(n)}$ be the $\varphi(n)$ distinct integers satisfying $1 \leqslant r_i \leqslant n$ and $\gcd(r_i, n) = 1$. Consider the $\varphi(n)$ integers

$$ar_1,\ ar_2,\ \ldots,\ ar_{\varphi(n)}.$$

We claim $\gcd(ar_i, n) = 1$ for each $1 \leqslant i \leqslant \varphi(n)$. Indeed, if p is a prime such that $p \mid ar_i$ for some $1 \leqslant i \leqslant \varphi(n)$ then $p \mid a$ or $p \mid r_i$. But $p \nmid n$ since $\gcd(a, n) = \gcd(r_i, n) = 1$.

Moreover we also claim $ar_i \not\equiv ar_j \bmod n$ if $i \neq j$. Indeed, assume $ar_i \equiv ar_j \bmod n$, then $n \mid a(r_i - r_j)$. But $\gcd(a, n) = 1$ so we have $n \mid r_i - r_j$, i.e., $r_i \equiv r_j \bmod n$. By our choice of r_i for $1 \leqslant i \leqslant \varphi(n)$, they are distinct if $i \neq j$.[1]

Therefore each ar_i is congruent to precisely one r_j.[2] In particular,

$$\begin{aligned} (ar_1)(ar_2)\cdots(ar_{\varphi(n)}) &\equiv r_1 r_2 \cdots r_{\varphi(n)} \bmod n \\ a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} &\equiv r_1 r_2 \cdots r_{\varphi(n)} \bmod n. \qquad (13.1) \end{aligned}$$

But $\gcd(r_1 r_2 \cdots r_{\varphi(n)}, n) = 1$ since $\gcd(r_i, n) = 1$ for each $1 \leqslant i \leqslant \varphi(n)$. We can cancel $r_1 r_2 \cdots r_{\varphi(n)}$ on both sides in Equation (13.1) then we have the result as desired. □

REMARK 13.1. We did use in the proof that if $a \equiv b \bmod n$ and $\gcd(a, n) = 1$, then $\gcd(b, n) = \gcd(a, n) = 1$.

EXAMPLE 13.2. Find the smallest positive integer in the congruence class of $2^{209} \bmod 15$.

SOLUTION. Recall $\varphi(15) = 8$ in Example 11.2 and $\gcd(2, 15) = 1$. We can apply Euler's theorem, then we have

$$2^8 \equiv 1 \bmod 15.$$

Also $209 = 26 \times 8 + 1$. So

$$\begin{aligned} 2^{209} &= (2^8)^{26} \times 2 \\ &\equiv 2 \bmod 15. \end{aligned}$$

□

Question: How do we compute $\varphi(n)$?

PROPOSITION 13.3. *Let $m, n \in \mathbb{Z}$ be positive coprime integers. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

[1] Another way to see this: Since $\gcd(a, n) = 1$, there is a unique $b \bmod n$ such that $ba \equiv 1 \bmod n$. Assume $ar_i \equiv ar_j \bmod n$, then $bar_i \equiv bar_j \bmod n$, which again implies $r_i = r_j$.

[2] How this works in the proof: By $\gcd(ar_i, n) = 1$ and $ar_i \equiv c \bmod n$ for some $c \in \mathbb{Z}$ up to n, we have $\gcd(c, n) = \gcd(ar_i, n) = 1$, meaning c is coprime with n. But we have selected all those integers up to n and coprime with n, i.e, the r_i's. So $ar_i \equiv c \equiv r_j \bmod n$.

Proof. Let $1 \leqslant a \leqslant mn$ satisfy $\gcd(a, mn) = 1$. Then there is a unique $1 \leqslant b \leqslant m$ and a unique $1 \leqslant c \leqslant n$ such that

$$a \equiv b \bmod m \text{ and } a \equiv c \bmod n.$$

Indeed, consider $a \equiv b \bmod m$ and $a \equiv b' \bmod m$ with $1 \leqslant b, b' \leqslant m$, $b, b' \in \mathbb{Z}$. $b \equiv a \equiv b' \bmod m \implies m \mid b - b'$. Since b, b' are restricted between 1 and m, we have $b' = b$. Also

$$\begin{aligned} \gcd(a, mn) = 1 &\implies \gcd(a, m) = 1 \\ &\implies \gcd(b, m) = \gcd(a, m) = 1. && \text{(by } a \equiv b \bmod m\text{)} \end{aligned}$$

Similarly, $\gcd(a, mn) = 1 \implies \gcd(c, n) = \gcd(a, n) = 1$. This shows given $1 \leqslant a \leqslant mn$ with $\gcd(a, mn) = 1$, we get unique $1 \leqslant b \leqslant m$ and $1 \leqslant c \leqslant n$ with $\gcd(b, m) = 1$ and $\gcd(c, n) = 1$.

On the other hand, if we have $1 \leqslant b \leqslant m$ and $1 \leqslant c \leqslant n$ satisfying $\gcd(b, m) = 1$ and $\gcd(c, n) = 1$, since $\gcd(m, n) = 1$, by Chinese remainder theorem, there is a unique $1 \leqslant a \leqslant mn$ such that

$$a \equiv b \bmod m \text{ and } a \equiv c \bmod n.$$

$\gcd(b, m) = 1$ and $a \equiv b \bmod m$ imply $\gcd(a, m) = \gcd(b, m) = 1$. Similarly $\gcd(c, n) = 1$ and $a \equiv c \bmod n$ imply $\gcd(a, n) = \gcd(c, n) = 1$. Hence $\gcd(a, mn) = 1$.

Therefore we have constructed a bijection between

$$\{a \in \mathbb{Z} : 1 \leqslant a \leqslant mn,\ \gcd(a, mn) = 1\}$$

and

$$\{(b, c) \in \mathbb{Z} \times \mathbb{Z} : 1 \leqslant b \leqslant m,\ 1 \leqslant c \leqslant n,\ \gcd(b, m) = \gcd(c, n) = 1\}.$$

Thus the two sets have the same cardinality (size), i.e., $\varphi(mn) = \varphi(m)\varphi(n)$. □

Remark 13.4. This proposition is not true without the coprime assumption on $m, n > 0$. For example, $\varphi(4) = 2 \neq 1 \times 1 = \varphi(2)\varphi(2)$.

Theorem 13.5. *Let $n \in \mathbb{Z}$, $n \geqslant 2$ and write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $k \in \mathbb{Z}$, $k > 0$, where p_i's are distinct primes with $e_i \geqslant 1$ for $1 \leqslant i \leqslant k$. Then*

$$\varphi(n) = (p_1 - 1)p_1^{e_1 - 1}(p_2 - 1)p_2^{e_2 - 1} \cdots (p_k - 1)p_k^{e_k - 1}.$$

Let us state a lemma before we prove Theorem 13.5.

Lemma 13.6. *Let e be a positive integer and p a prime. Then $\varphi(p^e) = (p - 1)p^{e-1}$.*

Proof. Let $a \in \mathbb{Z}$, $1 \leqslant a \leqslant p^e$. We know

$$\gcd(a, p^e) \neq 1 \iff p \mid a.$$

Thus the integers $1 \leqslant a \leqslant p^e$ such that $\gcd(a, p^e) \neq 1$ are multiples of p,

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

The number of multiples of p in this range is p^{e-1}. Hence

$$\begin{aligned} \varphi(p^e) &= p^e - p^{e-1} \\ &= (p - 1)p^{e-1}. \end{aligned}$$

□

PROOF (of Theorem 13.5). Since $p_1, p_2, \ldots, p_k$ are distinct primes, $p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$ are pairwise coprime. By Proposition 13.3, Euler φ-function is multiplicative.[3] We can repeatedly apply Proposition 13.3,

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})\\ &= \varphi(p_1^{e_1})\varphi(p_2^{e_2} \cdots p_k^{e_k})\\ &\vdots\\ &= \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k})\\ &= (p_1 - 1)p_1^{e_1-1}(p_2 - 1)p_2^{e_2-1} \cdots (p_k - 1)p_k^{e_k-1}.\end{aligned}$$

The last equality is due to Lemma 13.6 we just proved. □

EXAMPLE 13.7. Compute $\varphi(90)$.

SOLUTION.

$$\begin{aligned}\varphi(90) &= \varphi(2 \times 3^2 \times 5)\\ &= (2-1) \times (3-1)3 \times (5-1)\\ &= 24.\end{aligned}$$

□

Exercise.

13.1. Let $k, n \in \mathbb{Z}$, $k, n > 0$. If $k\varphi(n) = n - 1$ with $k \geqslant 2$ has integer solutions in n, then n is the product of at least four different odd primes.

13.2. Let $n \in \mathbb{Z}$ with $n > 0$. If $\varphi(n+3) = \varphi(n) + 2$, then either $n = 2p^\alpha$ or $n + 3 = 2p^\alpha$ for some prime p with $p \equiv 3 \bmod 4$ and $\alpha \in \mathbb{Z}$, $\alpha \geqslant 1$.

13.3. Let $a, b \in \mathbb{Z}$, $a, b > 0$ with $\gcd(a, b) = 1$. Show there exist $m, n \in \mathbb{Z}$, $m, n > 0$ such that $a^m + b^n \equiv 1 \bmod ab$.

– End of Part 1.[4]

[3] We will discuss multiplicative arithmetic functions in detail later in the course.

[4] Administrative announcement: Midterm 1 covers material up to this point.

Part 2

February to March, 2017

LECTURE 14

Day Fourteen

— 17.02.2017

Real application: RSA cryptosystem

Problem 14.1. Alice and Bob want to send secret messages but eavesdropper Eve cannot intercept the message.

Solution. Alice and Bob developed an elaborate code that only they share to encrypt and decrypt messages. This is called *symmetric key cryptosystem.* It requires both Alice and Bob to have the encoding and decoding data.

However this approach does not work on large scale. (e.g., banking system etc.) It requires either different schemes for every person (i.e., too much work, impractical) or to reuse scheme for different person (thus defeats its original purpose.)

The effective solution to this problem is *public key cryptosystem*: a cryptosystem where the encoding data and decoding data are different. The encoding data is called the **public key** and published to the world. The decoding key data is called the **private key** and is kept secret. The key ingredient of this approach is that it is difficult to determine the private key from the data of public key. □

Lemma 14.2. *Let n be a positive, square free integer. Let k be a positive integer such that $k \equiv 1 \bmod \varphi(n)$. Then $a^k \equiv a \bmod n$.*

Proof. A square free integer n is an integer $n = p_1p_2\cdots p_r$ with $p_1, p_2, \ldots, p_r$ distinct primes for $1 \leqslant i \leqslant r$, $r \in \mathbb{Z}$, $r > 0$. By the Chinese remainder theorem, for each $1 \leqslant i \leqslant r$,

$$a^k \equiv a \bmod n \iff a^k \equiv a \bmod p_i.$$

Indeed, ($\Rightarrow$) direction is by the definition of congruence so we can reduce the modulus n to its divisor p_i. ($\Leftarrow$) direction is actually due to the Chinese remainder theorem. For all r congruences

$$\begin{aligned} x &\equiv a \bmod p_1 \\ x &\equiv a \bmod p_2 \\ &\vdots \\ x &\equiv a \bmod p_r, \end{aligned} \tag{14.1}$$

there is a unique x_1 modulo $n = \prod_{i=1}^r p_i$ such that x_1 solves congruences in Equations (14.1). Similarly, for all r congruences

$$\begin{aligned} x &\equiv a^k \bmod p_1 \\ x &\equiv a^k \bmod p_2 \\ &\vdots \\ x &\equiv a^k \bmod p_r, \end{aligned} \tag{14.2}$$

there is a unique x_2 modulo $n = \prod_{i=1}^r p_i$ such that x_2 solves these congruences in Equations (14.2). Therefore $a^k \equiv x_2 \equiv x_1 \equiv a \bmod n$, i.e., a^k and a are in the same congruence class modulo n.

Fix some $1 \leqslant i \leqslant r$. We consider two cases.

(i) If $p_i \mid a$, then $p_i \mid a^k$. So $a^k \equiv 0 \equiv a \bmod p_i$.

(ii) If $p_i \nmid a$, then $\gcd(a, p_i) = 1$. By Fermat's little theorem, $a^{p_i - 1} \equiv 1 \bmod p_i$.

By our assumption, $k \equiv 1 \bmod \varphi(n)$ and n is square free,

$$\varphi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1),$$

we have $k \equiv 1 \bmod (p_i - 1)$ for each $1 \leqslant i \leqslant r$. Hence $k = 1 + m(p_i - 1)$ for some $m \in \mathbb{Z}$. Then

$$\begin{aligned} a^k &= a^{1+m(p_i-1)} \\ &\equiv a(a^{p_i-1})^m \bmod p_i \\ &\equiv a(1)^m \bmod p_i && \text{(by Fermat's little theorem[1])} \\ &\equiv a \bmod p_i. \end{aligned}$$

Then apply the argument at the beginning of this proof. □

The RSA cryptosystem is one of the first and still widely used public key cryptosystem.

RSA cryptosystem set-up (Rivest–Shamir–Adleman, 1977; Cocks, 1973[2]):

- Choose two large primes p, q and compute $n = pq$;
- Compute $\varphi(n) = (p-1)(q-1)$;
- Choose $1 \leqslant e \leqslant \varphi(n)$ with $\gcd(e, \varphi(n)) = 1$;
- Compute the multiplicative inverse of e modulo $\varphi(n)$, i.e., $1 \leqslant d \leqslant \varphi(n)$ such that $de \equiv 1 \bmod \varphi(n)$;
- Then the *public key* is (e, n) and the *private key* is (d, n).

[1] What if $m < 0$? (It cannot happen since $k > 0$.)

[2] Not declassified until 1997.

LECTURE 15

Day Fifteen

— 20.02.2017

Recall the set-up of RSA cryptosystem from last time,

- p and q are two large primes; compute $n = pq$;
- An integer $1 \leqslant e \leqslant \varphi(n)$, is coprime with $\varphi(n) = (p-1)(q-1)$;
- Compute $1 \leqslant d \leqslant \varphi(n)$, the multiplicative inverse of e modulo $\varphi(n)$ such that $de \equiv 1 \bmod \varphi(n)$;
- (e, n) is the public key and (d, n) is the private key.

Encryption: Say $m \in \mathbb{Z}$, $1 \leqslant m \leqslant n$, is the message. Compute the smallest positive (or nonnegative) integer c in the residue class of $m^e \bmod n$. This c is the coded message.

Decryption: Since $de \equiv 1 \bmod \varphi(n)$, Lemma 14.2 from last lecture gives

$$\begin{aligned} c^d &= m^{ed} \\ &\equiv m \bmod n. \end{aligned}$$

So m is the smallest nonnegative integer in the residue class of c^d.

Remark 15.1. Why is this secure? To compute d from e, one needs to first compute $\varphi(n)$. For this, one also needs to factor n. This is difficult (as of now).

Remark 15.2. Currently, the largest RSA successfully factored was an n with 232 digits in 2009. It took hundreds of computers two years. In practice, RSA uses n with between 300 and 1200 digits (or 1024 bits and 4096 bits).

Remark 15.3. In 2012, Lenstra et al. gathered millions of public keys and used Euclidean algorithm to computed gcd of pairs of n's. They successfully factored 0.2% of the keys they gathered. They concluded people were reusing primes.

Technical details: How do we generate *large primes* in the first place? In practice, we generate integers that are *probable primes*, i.e., integers that are prime with a probability greater than a fixed probability (on the same order, say, a server will be hit by a tornado or a lightening, twice.)

One such algorithm is (roughly) as follows:

- Choose a random large odd number b;
- Check if b is divisible by a list of small primes. If so, start again with $b + 2$; if not, continue to the next step;
- Perform several iterations of the Miller–Rabin test. If b fails one of these tests, start again with $b + 2$; if not, then b is a probable prime.

Remark 15.4. The prime number theorem says that

$$|\{p \leqslant x : p \text{ is prime}\}| \sim \frac{x}{\log x}.$$

So primes have density roughly "$\frac{1}{\log x}$ around x." One expects a prime in the interval $b \leqslant x \leqslant b + \log b$. If b is 300 digits, $\log b \approx 690$. We should expect about 350 iterations using the above algorithm.

Miller–Rabin test: Note if p is prime, for $x \in \mathbb{Z}$ such that $x^2 \equiv 1 \bmod p$, x is its own multiplicative inverse if and only if $x \equiv \pm 1 \bmod p$. This is not necessarily true for composite modulus, e.g., we know $3^2 \equiv 1 \bmod 8$ but $3 \not\equiv \pm 1 \bmod 8$.

Say p is an odd prime with $p-1 = 2^k m$, where $k \geqslant 1$ and m odd positive integer. Take $1 \leqslant a \leqslant p-1$, then by Fermat's little theorem,

$$a^{2^k m} \equiv a^{p-1} \equiv 1 \bmod p.$$

By our observation from the above quadratic congruence modulo p,

$$a^{2^k m} \equiv \left(a^{2^{k-1} m}\right)^2 \equiv 1 \mod p \implies$$
$$a^{2^{k-1} m} \equiv \pm 1 \bmod p.$$

If $a^{2^{k-1} m} \equiv 1 \bmod p$ and $k > 1$, we repeat and get

$$a^{2^{k-2} m} \equiv 1 \bmod p.$$

Continue this we obtain that either

$$a^m \equiv 1 \bmod p \text{ (take away all powers of 2)}$$

or

$$a^{2^r m} \equiv -1 \bmod p \text{ for some } 0 \leqslant r \leqslant k-1.$$

We can turn the above observation regarding a prime p into a contrapositive argument. For any odd integer $n > 2$, writing $n-1 = 2^{k-1} m$ with m odd, $m \in \mathbb{Z}$, $m > 0$, if there is an integer $1 \leqslant a \leqslant n-1$ such that

$$a^m \not\equiv 1 \mod n$$

and

$$a^{2^r m} \not\equiv -1 \bmod n \text{ for any } 0 \leqslant r \leqslant k-1,$$

then n is not prime. Hence the Miller–Rabin test:

- Choose a random $1 \leqslant a \leqslant n-1$ and compute $a^m \bmod n$ and $a^{2^r m} \bmod n$ for each $0 \leqslant r \leqslant k-1$;
- Check against the aforementioned contrapositive argument about n;
- For a single Miller–Rabin test, more than $\frac{3}{4}$ of the choices $1 \leqslant a \leqslant n-1$ will show n is composite under Miller–Rabin test if n is indeed composite.

Question: How do we compute large primes *for fun*?

Definition 15.5. A **Mersenne prime** is a prime of the form $2^p - 1$ with p prime.

Example 15.6. $2^2-1=3$, $2^3-1=7$, $2^5-1=31$, $2^7-1=127$ are all Mersenne primes. However $2^{11}-1 = 23 \times 89$ is not a Mersenne prime. $2^{13}-1 = 8191$ is Mersenne.

The largest known prime (as of now, also Mersenne) is

$$2^{74,207,281} - 1$$

found in 2016 and it has 22,338,618 digits. The discovery of this Mersenne prime was a result of GIMPS (Great Internet Mersenne Prime Search).

LECTURE 16

Day Sixteen

— 22.02.2017

Recall from last time, a Mersenne prime is a prime of the form $2^p - 1$ with p prime.

CONJECTURE 16.1. *There are infinitely many Mersenne primes.*

DEFINITION 16.2. A **Fermat prime** is a prime of the form $2^{2^n} + 1$ with $n \in \mathbb{Z}$, $n \geqslant 0$.

EXAMPLE 16.3. $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, $2^{2^4} + 1 = 65537$ are all Fermat primes. But Euler found $2^{2^5} + 1 = 641 \times 6700417$.

So far we do not know whether there are other Fermat primes. It is believed these are the only ones.

Also from last time, we saw that if p is prime, then[1]

$$a^2 \equiv 1 \bmod p \iff a \equiv \pm 1 \bmod p.$$

So if $a^2 \equiv 1 \bmod p$ for $1 \leqslant a \leqslant p-1$, then $a = 1$ or $a = p-1$. We also know from our discussion of multiplicative inverse that if $1 \leqslant a \leqslant p-1$, $\gcd(a,p) = 1$, then there is a unique $1 \leqslant b \leqslant p-1$ such that $ab \equiv 1 \bmod p$. If $a^2 \equiv 1 \bmod p$, it means $b = a$, then we have $b = 1$ or $p-1$. Consequently, we have the following lemma.

LEMMA 16.4. *Let p be an odd prime, $p \geqslant 5$. For each $2 \leqslant a \leqslant p-2$, there is a unique $2 \leqslant b \leqslant p-2$ such that $ab \equiv 1 \bmod p$ and $b \neq a$.*

PROOF. By the discussion right before we stated this lemma, it follows immediately. □

EXAMPLE 16.5. For a prime $p = 7$, modulo 7, we have

$$\begin{aligned}
1 \times 1 = 1 \ \ &\equiv 1 \bmod 7\\
2 \times 4 = 8 \ \ &\equiv 1 \bmod 7\\
3 \times 5 = 15 &\equiv 1 \bmod 7\\
6 \times 6 = 36 &\equiv 1 \bmod 7.
\end{aligned}$$

THEOREM 16.6 (Wilson's theorem). *Let p be a prime, then $(p-1)! \equiv -1 \bmod p$.*

PROOF. If $p = 2$, then $(p-1)! = 1! \equiv -1 \bmod 2$.

If $p = 3$, then $(p-1)! = 2! \equiv -1 \bmod 3$.

If $p \geqslant 5$, by Lemma 16.4, there is a unique $2 \leqslant b \leqslant p-2$ for each $2 \leqslant a \leqslant p-2$ such that $ab \equiv 1 \bmod p$ with $b \neq a$. Hence the numbers $2, 3, \ldots, p-2$ can be grouped into $\left(\frac{p-3}{2}\right)$ pairs of (a,b), $2 \leqslant a, b \leqslant p-2$ such that $ab \equiv 1 \bmod p$, meaning the elements of the product $2 \cdot 3 \cdot \cdots \cdot (p-2)$ can

[1] Proof. ($\Rightarrow$) If $a^2 \equiv 1 \bmod p$ then $p \mid (a+1)(a-1)$. Therefore either $p \mid a+1$ or $p \mid a-1$ since p is prime, i.e., $a \equiv \pm 1 \bmod p$. ($\Leftarrow$) If $a \equiv \pm 1 \bmod p$, then $a \cdot a \equiv (\pm 1) \cdot (\pm 1) \bmod p$, i.e., $a^2 \equiv 1 \bmod p$.

Alternative proof: p is prime so the ring $(\mathbb{Z}_p, +, \times)$ is a finite field $\mathbb{F}_p$, hence it is an integral domain. In this integral domain $\mathbb{Z}_p$, we have $x^2 = 1 \iff (x+1)(x-1) = 0 \iff x+1 = 0$ or $x-1 = 0$, i.e., $x = \pm 1$.

be reordered so that

$$\begin{aligned}(p-1)! &= 1\cdot(2\cdot 3\cdot \cdots \cdot p-2)\cdot(p-1)\\ &\equiv 1\cdot(\underbrace{1\cdot 1\cdot \cdots \cdot 1}_{\frac{p-3}{2}\text{ copies}})\cdot\,(p-1) \bmod p\\ &\equiv p-1 \bmod p\\ &\equiv -1 \quad \bmod p.\end{aligned}$$

We completed the proof. □

Proposition 16.7. *If $n\in\mathbb{Z}$, $n\geqslant 2$ such that $(n-1)!\equiv -1 \bmod n$, then n is prime.*

Proof. Recall $a\equiv b \bmod n$ then $\gcd(a,n)=\gcd(b,n)$. Therefore

$$(n-1)!\equiv -1 \bmod n \implies \gcd((n-1)!,n)=\gcd(-1,n).$$

But $\gcd(-1,n)=1$, and $d\mid(n-1)!$ for each $2\leqslant d\leqslant n-1$, $d\in\mathbb{Z}$. It follows that $d\nmid n$ for $2\leqslant d\leqslant n-1$ since $\gcd((n-1)!,n)=1$. Then the only possible divisors of n is just 1 and n, hence n is prime. □

Exercises.

16.1. Find the residue of 50! modulo 47^2. (*Hint*: $\frac{50!}{47}\equiv 41 \bmod 47$.)

16.2. Let p be an odd prime. Show that

$$1^2\cdot 3^2\cdot\cdots\cdot(p-2)^2\equiv(-1)^{\frac{p+1}{2}} \bmod p,$$
$$2^2\cdot 4^2\cdot\cdots\cdot(p-1)^2\equiv(-1)^{\frac{p+1}{2}} \bmod p.$$

16.3. Let $a_1,a_2,\ldots,a_n$ and $b_1,b_2,\ldots,b_n$ are two complete residue systems modulo n. Show that
(a) if $2\mid n$, then $a_1+b_1,a_2+b_2,\ldots,a_n+b_n$ is not a complete residue system modulo n;
(b) if $n>2$, then $a_1b_1,a_2b_2,\ldots,a_nb_n$ is not a complete residue system modulo n.

16.4. Show $61!+1\equiv 0 \bmod 71$ and $63!+1\equiv 0 \bmod 71$. (*Hint*: First show if $(-1)^r r!\equiv 1 \bmod p$ for an odd prime p and $1\leqslant r\leqslant p-1$, $r\in\mathbb{Z}$, then $(p-r-1)!+1\equiv 0 \bmod p$.)

16.5. Let $p>3$ be an odd prime satisfying

$$1+\frac{1}{2}+\cdots+\frac{1}{p-1}+\frac{1}{p}=\frac{a}{p^b}$$

with $a,b\in\mathbb{Z}$, $a,b>0$ and $\gcd(a,b)=1$. Show that $p^3\mid a-b$.

LECTURE 17

Day Seventeen

— 27.02.2017

Quadratic Residues: When an integer is a square modulo p with p prime.

Definition 17.1. Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$. We say a is a **quadratic residue modulo** n if $\exists\, x \in \mathbb{Z}$ such that

$$x^2 \equiv a \bmod p.$$

Otherwise we say a is a **quadratic nonresidue modulo** n.

Remark 17.2. Let a, n be the same as in Definition 17.1.

- If $a \equiv b \bmod n$, then
$$a \text{ is a quadratic residue modulo } n \iff b \text{ is a quadratic residue modulo } n.$$
- If $x^2 \equiv a \bmod n$ and $\gcd(a, n) = 1$, then $\gcd(x, n) = 1$. Indeed,
$$\begin{aligned} \gcd(a,n) > 1 &\iff \exists \text{ prime } p \text{ such that } p \mid x \text{ and } p \mid n \\ &\iff \exists \text{ prime } p \text{ such that } p \mid x^2 \text{ and } p \mid n \\ &\iff \gcd(x^2, n) \geqslant p > 1 \\ &\iff \gcd(a, n) \geqslant p > 1. \end{aligned}$$

Example 17.3. Find all quadratic residues modulo 7.

Solution. Note that if $x^2 \equiv a \bmod 7$ and $x \equiv r \bmod 7$ then $r^2 \equiv a \bmod 7$. Indeed, $x \equiv r \bmod 7 \implies x = 7q + r$ for some unique $q, r \in \mathbb{Z}$, $0 \leqslant r < 7$ by division algorithm. Therefore

$$\begin{aligned} x^2 &= (7q + r)^2 \\ &\equiv r^2 \bmod 7. \end{aligned}$$

We can loop over $r \in \{1, 2, \ldots, 6\}$ to compute residue classes modulo 7. Note that $r = 0$ is not included since $\gcd(r, 7) = \gcd(x, 7) = 1$ by Remark 17.2.

$$\begin{aligned} 1^2 &\equiv 1 \bmod 7 \\ 2^2 &\equiv 4 \bmod 7 \\ 3^2 &\equiv 2 \bmod 7 \\ 4^2 &\equiv 2 \bmod 7 \\ 5^2 &\equiv 4 \bmod 7 \\ 6^2 &\equiv 1 \bmod 7. \end{aligned}$$

So we see that $a \in \mathbb{Z}$ with $\gcd(a, 7) = 1$ is a quadratic residue modulo 7 if and only if $a \equiv 1, 2,$ or $4 \bmod 7$. □

Remark 17.4. We could have seen easily that $6^2 \equiv 1 \bmod 7$ since $6^2 \equiv (-1)^2 = 1 \bmod 7$. Similarly, $5^2 \equiv (-2)^2 = 2^2 \equiv 4 \bmod 7$. In general, if $\gcd(a, n) = 1$, $n > 0$ and $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod n$, then $(n - x)^2 \equiv (-x)^2 = x^2 \equiv a \bmod n$.

Proposition 17.5. *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. The congruence $x^2 \equiv a \bmod p$ either has no solutions in $x \in \mathbb{Z}$ or has precisely two incongruent solutions modulo p.*

Sketch of Proof. It suffices to show that if $x^2 \equiv a \bmod p$ has a solution $x \in \mathbb{Z}$, then it has exactly two solutions. Obviously, if $x^2 \equiv a \bmod p$ then $(-x)^2 \equiv a \bmod p$. We can show that $x \not\equiv -x \bmod p$.[1] So when it has solutions, it has at least two two incongruent solutions $\pm x$ modulo p.

On the other hand, for any other solution $y \in \mathbb{Z}$ with $y^2 \equiv a \bmod p$, we have

$$\begin{aligned} y^2 &\equiv a \mod p \\ &\equiv x^2 \bmod p \\ \iff p &\mid (y^2 - x^2) \\ \iff p &\mid y + x \text{ or } p \mid y - x \qquad\qquad \text{(by } p \text{ is prime)} \end{aligned}$$

i.e., either $y \equiv x \bmod p$ or $y \equiv -x \bmod p$. So it has at most two solutions. Hence when $x^2 \equiv a \bmod p$ has solutions, it has exactly two solutions. ■

Remark 17.6. It fails for composite moduli, e.g, for $n = 8$, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. For $n = 15$, $1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \bmod 15$. In both cases the quadratic congruence has four incongruent solutions.

Exercises.

17.1. If $5x^2 \equiv 1 \bmod p$ with p prime, show 5 is a quadratic residue modulo p.

[1] Assume the contrary, $x \equiv -x \bmod p \implies p \mid 2x$. But p is odd and $\gcd(x, p) = 1$, a contradiction.

LECTURE 18

Day Eighteen

— 01.03.2017

Proposition 18.1. *Let p be an odd prime. There are* ***exactly*** $\frac{p-1}{2}$ *quadratic residues modulo p and the same amount of quadratic nonresidues modulo p.*

Proof. For any $x \in \{1, 2, \ldots, p-1\}$, $\exists\ a \in \{1, 2, \ldots, p-1\}$ such that $x^2 \equiv a \bmod p$.

On the other hand, we saw in Proposition 17.5 if $a \in \{1, 2, \ldots, p-1\}$ is a quadratic residue, then there are exactly two different $x \in \{1, 2, \ldots, p-1\}$ such that $x^2 \equiv a \bmod p$. As x ranges over the elements of the set $\{1, 2, \ldots, p-1\}$, the congruence classes of x^2 take $\frac{p-1}{2}$ values. Thus there are $\frac{p-1}{2}$ quadratic residues. And there are $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ quadratic nonresidues. □

Example 18.2. We saw that 1, 2, 4 are all incongruent quadratic residues modulo 7 and 3, 5, 6 are quadratic nonresidues modulo 7 in Example 17.3.

Example 18.3. Note Proposition 18.1 fails for composite moduli, e.g., modulo 8. Any $x \in \mathbb{Z}$ with $\gcd(x, 8) = 1$ satisfies $x^2 \equiv 1 \bmod 8$; 1 is a quadratic residue modulo 8. But we saw in Remark 17.6, 3, 5, 7 are quadratic nonresidues modulo 8.

Definition 18.4. Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then the **Legendre symbol** for p and a, denoted $\left(\frac{a}{p}\right)$ is defined by

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

Example 18.5. We rephrase Example 17.3 in the language of Legendre symbol modulo 7.

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$$
$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{5}{7}\right) = -1.$$

Remark 18.6. The Legendre symbol gives no information about computing the solutions to $x^2 \equiv a \bmod p$, only whether or not a solution exists.

Theorem 18.7 (Euler's criterion). *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

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

Proof. First assume $\left(\frac{a}{p}\right) = 1$. By Definition 18.4, there is an $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod p$ and $p \nmid x$. Then

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \left(x^2\right)^{\frac{p-1}{2}} && \bmod p \\ &\equiv x^{p-1} && \bmod p \\ &\equiv 1 && \bmod p. \qquad \text{(by Fermat's little theorem)} \end{aligned}$$

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

Now assume $\left(\frac{a}{p}\right) = -1$. For any $b \in \{1, 2, \ldots, p-1\}$, we have $\gcd(b, p) = 1$. There is a unique $c \in \{1, 2, \ldots, p-1\}$ such that $bc \equiv a \bmod p$. Further by $\left(\frac{a}{p}\right) = -1$, a is a quadratic nonresidue modulo p, hence for each b, the associated c cannot be the same as b. We can pair up the $p-1$ elements $1, 2, \ldots, p-1$ into $\left(\frac{p-1}{2}\right)$ pairs (b, c), $\forall\ b, c \in \{1, 2, \ldots, p-1\}$ such that $bc \equiv a \bmod p$. Then

$$\begin{aligned}(p-1)! &\equiv \underbrace{a \cdot a \cdot \cdots \cdot a}_{\frac{p-1}{2} \text{ copies}} \bmod p \\ &\equiv a^{\frac{p-1}{2}} \bmod p.\end{aligned}$$

At the same time, by Wilson's theorem, $(p-1)! \equiv -1 \bmod p$. So we have $\left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}} \bmod p$. □

Theorem 18.8. *Let p be an odd prime. Then*

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

Proof. By Euler's criterion,

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

Since both sides are ± 1 and $1 \not\equiv -1 \bmod p$ (p is an odd prime; otherwise $p \mid 2$), we have

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

□

Remark 18.9. Without Euler's criterion, it is easy to see

$$\text{quadratic residue} \times \text{quadratic residue} = \text{quadratic residue},$$

not too hard to get

$$\text{quadratic residue} \times \text{quadratic nonresidue} = \text{quadratic nonresidue}.$$

However it is not obvious that

$$\text{quadratic nonresidue} \times \text{quadratic nonresidue} = \text{quadratic residue}.$$

Day Nineteen

— 03.03.2017

PROPOSITION 19.1. *Let p be an odd prime and let $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then*

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

PROOF. Since $p \nmid a$ and $p \nmid b$, we have $p \nmid ab$. By Euler's criterion,

$$\begin{aligned} \left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} &&\mod p \\ &\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} &&\mod p \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) &&\mod p. \end{aligned}$$

Since $\left(\frac{ab}{p}\right)$, $\left(\frac{a}{p}\right)$ and $\left(\frac{b}{p}\right)$ are all ±1, p is an odd prime, we have

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

□

THEOREM 19.2. *Let p be an odd prime. Then*

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

PROOF. Let $s = \frac{p-1}{2}$ and consider the equalities

$$\begin{aligned} 1 &= (-1)(-1) \\ 2 &= (+2)(-1)^2 \\ 3 &= (-3)(-1)^3 \\ 4 &= (+4)(-1)^4 \\ &\vdots \\ s &= (\pm s)(-1)^s. \end{aligned} \tag{19.1}$$

The plus or minus sign in the last term of Equations (19.1) depends on whether s is even or odd. Multiply the left hand sides and right hand sides of Equations (19.1) respectively, we have

$$s! = \Big((-1)(+2)(-3)\cdots(\pm s)\Big)(-1)^{1+2+\cdots+s},$$

where the positive elements in the product $(-1)(+2)(-3)\cdots(\pm s)$ are all the even integers between 1 and $s = \frac{p-1}{2}$ while the negative elements are negations of odd integers between 1 and $s = \frac{p-1}{2}$.

Notice that if $1 \leqslant a \leqslant \frac{p-1}{2}$ is odd then $p - a$ is even, and $p - a \equiv -a \mod p$ for $\frac{p+1}{2} \leqslant p - a \leqslant p - 1$. Moreover,

$$\left\{p - a : 1 \leqslant a \leqslant \frac{p-1}{2},\ a \text{ is odd}\right\} = \left\{b : \frac{p+1}{2} \leqslant b \leqslant p - 1,\ b \text{ is even}\right\},$$

where a, b of the two sets are symmetric with respect to the midpoint number $\frac{p}{2} \in \mathbb{R}$. Thus the product

$$\begin{aligned}(-1)(+2)(-3)\cdots(\pm s) &\equiv 2 \cdot 4 \cdot \cdots \cdot (p-3)(p-1) \bmod p \\ &\equiv (2\cdot 1)(2 \cdot 2)\cdots(2\cdot(s-1))(2\cdot s) \bmod p \\ &\equiv 2^s s! \bmod p.\end{aligned}$$

Next $1+2+\cdots+s = \frac{s(s+1)}{2}$. Therefore we have

$$s! \equiv 2^s s! (-1)^{\frac{s(s+1)}{2}} \bmod p.$$

Since $p \nmid s!$, we can cancel out (by Proposition 10.8) $s!$ on both sides to get

$$\begin{aligned}1 &\equiv 2^s(-1)^{\frac{s(s+1)}{2}} \bmod p \implies \\ 2^s &\equiv (-1)^{\frac{s(s+1)}{2}} \bmod p.\text{[1]}\end{aligned}$$

But $s = \frac{p-1}{2}$ and $\gcd(2,p) = 1$, so by Euler's criterion,

$$\begin{aligned}2^s &= 2^{\frac{p-1}{2}} \\ &\equiv \left(\frac{2}{p}\right) \bmod p.\end{aligned}$$

Hence

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

The equality follows from that they are ±1 on both sides of the above congruence and p is an odd prime.

Finally,

$$\begin{aligned}(-1)^{\frac{s(s+1)}{2}} &= \begin{cases} 1 & \text{if } s = 4k \quad \text{ or } s = 4k+3 \text{ for some } k \in \mathbb{Z}, \\ -1 & \text{if } s = 4k+1 \text{ or } s = 4k+2 \text{ for some } k \in \mathbb{Z}.\end{cases} \\ &= \begin{cases} 1 & \text{if } p = 8k+1 \text{ or } p = 8k+7 \text{ for some } k \in \mathbb{Z}, \\ -1 & \text{if } p = 8k+3 \text{ or } p = 8k+5 \text{ for some } k \in \mathbb{Z}.\end{cases}\end{aligned}$$

□

EXAMPLE 19.3. Consider the prime 257. It satisfies

$$\begin{aligned}257 &= 240 + 17 \\ &\equiv 17 \bmod 8 \\ &\equiv 1 \quad \bmod 8.\end{aligned}$$

Thus $\left(\frac{2}{p}\right) = 1$, i.e., 2 is a quadratic residue modulo 257.

Question: For which primes is (-2) a quadratic residue?

Let p be an odd prime, by Proposition 19.1,

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

REMARK 19.4. Theorem 18.8 and Theorem 19.2 are called the **first supplement** and the **second supplement to quadratic reciprocity** respectively.

[1] Multiply both sides by $\frac{s(s+1)}{2}$ and note that $s(s+1)$ is even. This trick will be used again so we can move one term to the other side when we consider quadratic reciprocity law.

LECTURE 20

Day Twenty

— 06.03.2017

Quadratic reciprocity (QR law)

THEOREM 20.1. *Let p, q be odd primes. Then*

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

The proof itself takes more than a single lecture and we shall see some numerical evidences before the proof is given.

EXAMPLE 20.2. Is 5 quadratic residue modulo 77797?

SOLUTION. No. Note that 77797 is an odd prime as is 5. By quadratic reciprocity (Theorem 20.1),

$$\left(\frac{5}{77797}\right)\left(\frac{77797}{5}\right) = (-1)^{\frac{5-1}{2}\times\frac{77797-1}{2}} = 1.$$

We do not need to compute $\frac{77797-1}{2}$ since $\frac{5-1}{2}$ is even.

Therefore

$$\begin{aligned}\left(\frac{5}{77797}\right) &= \left(\frac{77797}{5}\right)\\ &= \left(\frac{2}{5}\right) && \text{(by } 77797 \equiv 2 \bmod 5\text{)}\\ &= -1.\end{aligned}$$

Hence 5 is not a quadratic residue modulo 77797. □

EXAMPLE 20.3. Determine whether or not (-30) is a quadratic residue modulo 257.

SOLUTION. 257 is an odd prime. We can break $\left(\frac{-30}{257}\right)$ into the product of several Legendre symbols by Proposition 19.1,

$$\left(\frac{-30}{257}\right) = \left(\frac{-1}{257}\right)\left(\frac{2}{257}\right)\left(\frac{3}{257}\right)\left(\frac{5}{257}\right).$$

By the first supplement to quadratic reciprocity (Theorem 18.8), $\left(\frac{-1}{257}\right) = 1$ since $257 \equiv 1 \bmod 4$. By the second supplement to quadratic reciprocity (Theorem 19.2), $\left(\frac{2}{257}\right) = 1$ since $257 \equiv 1 \bmod 8$. We also know[1] $\left(\frac{3}{257}\right) = -1$ since $257 \equiv 5 \bmod 12$, not $\pm 1 \bmod 12$; $\left(\frac{5}{257}\right) = -1$ since $257 \equiv 2 \bmod 5$, not 1 or 4 mod 5.

Therefore

$$\left(\frac{-30}{257}\right) = 1 \times 1 \times (-1) \times (-1) = 1,$$

i.e., -30 is a quadratic residue modulo 257. □

EXAMPLE 20.4. Determine whether or not 193 is a quadratic residue modulo 293.

[1] These are based on exercise problems in [**Str01**, §4.3]. See Problems 35, 36.

SOLUTION. 193 and 273 are both odd primes. By quadratic reciprocity,

$$\left(\frac{193}{273}\right)\left(\frac{273}{193}\right) = (-1)^{\frac{193-1}{2}\times\frac{273-1}{2}} = 1.$$

And

$$\left(\frac{273}{193}\right) = \left(\frac{273-193}{193}\right) = \left(\frac{80}{193}\right) = \left(\frac{2^4\times 5}{193}\right) = \left(\frac{5}{193}\right) = -1.$$[2]

Therefore $\left(\frac{193}{273}\right) = \frac{1}{-1} = -1$. Hence 193 is not a quadratic residue modulo 273. □

The proof of quadratic reciprocity presented here is due to G. Rousseau [**Rou91**], however treated in such an elementary way that the language of abstract algebra is not used. This proof is also different from the lattice points counting proof used in [**Str01**]. The rough idea of this proof is to consider multiplying together "half" of the elements of $1 \leqslant a \leqslant pq$ with $\gcd(a, pq) = 1$. In three ways, using Chinese remainder theorem, we show that these three different ways are equal modulo pq up to a sign. We then show these differences in signs are $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ and $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ using Euler's criterion.

NOTATION 20.5. Let $\mathcal{A}$ be some finite subset of $\mathbb{Z}$. We use $\prod_{a\in\mathcal{A}} a$ to denote the product of all elements in $\mathcal{A}$, e.g, $n! = \prod_{1\leqslant j\leqslant n} j$.

PROOF (of Theorem 20.1, quadratic reciprocity). Let $\mathcal{A} = \left\{a \in \mathbb{Z} : 1 \leqslant a < \frac{pq}{2}, \gcd(a, pq) = 1\right\}$. Let $R = \prod_{a\in\mathcal{A}} a$. We want to evaluate $R \bmod p$ and $R \bmod q$. R can be written explicitly as

$$R = \left(\frac{1}{1\cdot q\cdot \cdots \cdot \left(\frac{p-1}{2}\right) q}\right)\Big(\overbrace{1\cdot 2\cdot \cdots \cdot (p-1)}^{(p-1)\text{ terms}}\Big)\Big(\overbrace{(p+1)\cdot(p+2)\cdot \cdots \cdot (p+(p-1))}^{(p-1)\text{ terms}}\Big)\cdots$$

$$\left(\overbrace{\left(p\left(\frac{q-1}{2}\right)+1\right)\cdot\left(p\left(\frac{q-1}{2}\right)+2\right)\cdot \cdots \cdot\left(p\left(\frac{q-1}{2}\right)+\frac{p-1}{2}\right)}^{\text{only }\frac{p-1}{2}\text{ terms}}\right)$$

$$\begin{aligned} &= \frac{\left(\prod_{i=1}^{p-1} i\right)\left(\prod_{i=1}^{p-1} p+i\right)\cdots\left(\prod_{i=1}^{p-1} p\left(\frac{q-3}{2}\right)+i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} p\left(\frac{q-1}{2}\right)+i\right)}{\prod_{i=1}^{\frac{p-1}{2}} iq} \qquad (20.1)\\ &= \frac{\left(\prod_{j=0}^{\frac{q-3}{2}}\prod_{i=1}^{p-1} pj+i\right)\left(\prod_{i=1}^{\frac{p-1}{2}} p\left(\frac{q-1}{2}\right)+i\right)}{\prod_{i=1}^{\frac{p-1}{2}} i}. \end{aligned}$$

Here we have written in the numerator the product of all integers between 1 and $\frac{pq-1}{2}$ that are coprime with p, and in the denominator all multiples of q in the same range.[3] Denote the numerator and the denominator N and D respectively in Equation (20.1). We have $DR = N$. (To be continued.)

[2] Again by quadratic reciprocity, $\left(\frac{5}{193}\right)\left(\frac{193}{5}\right) = (-1)^{\frac{5-1}{2}\times\frac{193-1}{2}} = 1 \implies \left(\frac{5}{193}\right) = \frac{1}{\left(\frac{193}{5}\right)} = \frac{1}{-1} = -1$ since $\left(\frac{193}{5}\right) = \left(\frac{3}{5}\right) = -1$.

[3] As in $\prod_{i=1}^{\frac{p-1}{2}} p\left(\frac{q-1}{2}\right)+i$ of Equation (20.1), we needed to calculate m, n in $\left(\prod_{i=1}^{m} pn+i\right)$ in order to write down the correct last term in the numerator. To get $n = \frac{q-1}{2}$, consider the largest $n \in \mathbb{Z}$ such that $np \leqslant \frac{pq-1}{2}$. It implies $n \leqslant \frac{pq-1}{2p} = \frac{q}{2} - \frac{1}{2p} = \lfloor\frac{q}{2}\rfloor + \frac{1}{2} - \frac{1}{2p}$ since q is odd. And $p > 1$, hence $\frac{1}{2} - \frac{1}{2p} \in \left(0, \frac{1}{2}\right)$. Therefore $n = \lfloor\frac{q}{2}\rfloor = \frac{q-1}{2}$ as desired. As for m, consider the largest $m \in \mathbb{Z}$ such that $p\left(\frac{q-1}{2}\right) + m < \frac{pq}{2}$. Then $m < \frac{p}{2}$. Hence $m = \lfloor\frac{p}{2}\rfloor = \frac{p-1}{2}$.

LECTURE 21

Day Twenty-One

— 08.03.2017

Proof (of Theorem 20.1, quadratic reciprocity, continued). The denominator in Equation (20.1)

$$\begin{aligned} D &= \prod_{i=1}^{\frac{p-1}{2}} iq \\ &= q^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} i \\ &= \left(\frac{p-1}{2}\right)!\, q^{\frac{p-1}{2}}. \end{aligned}$$

Thus $DR = N$ implies

$$\begin{aligned} \left(\frac{p-1}{2}\right)!\, q^{\frac{p-1}{2}} R &\equiv \left(\prod_{j=0}^{\frac{q-3}{2}} \prod_{i=1}^{p-1} i\right) \left(\prod_{i=1}^{\frac{p-1}{2}} i\right) \bmod p \\ &\equiv \left(\prod_{i=1}^{p-1} i\right)^{\frac{q-1}{2}} \left(\prod_{i=1}^{\frac{p-1}{2}} i\right) \bmod p \\ &\equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \bmod p. \end{aligned} \tag{21.1}$$

Since $p \nmid \left(\frac{p-1}{2}\right)!$, we can cancel $\left(\frac{p-1}{2}\right)!$ from both sides of Equation (21.1) . Further by Euler's criterion, we have $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \bmod p$. Then Equation (21.1) becomes

$$\left(\frac{q}{p}\right) R \equiv (p-1)!^{\frac{q-1}{2}} \bmod p.$$

By a symmetric argument, switching the roles of p and q, we get

$$\left(\frac{p}{q}\right) R \equiv (q-1)!^{\frac{p-1}{2}} \bmod q.$$

Now let B be the set of $1 \leqslant b \leqslant pq$ with $\gcd(b, pq) = 1$ such that

$$\begin{aligned} &b \equiv i \bmod p \text{ for some } 1 \leqslant i \leqslant p-1, \text{ and} \\ &b \equiv j \bmod q \text{ for some } 1 \leqslant j \leqslant \frac{q-1}{2}. \end{aligned}$$

By Chinese remainder theorem, there is a unique $1 \leqslant b \leqslant pq-1$ coprime with pq for every such pair (i, j). Set $Q = \prod_{b \in \mathcal{B}} b$, where

$$\mathcal{B} = \left\{ 1 \leqslant b \leqslant pq-1 : b \equiv i \bmod p \text{ for } 1 \leqslant i \leqslant p-1 \text{ and } b \equiv j \bmod q \text{ for } 1 \leqslant j \leqslant \frac{q-1}{2} \right\}.$$

Thus

$$
\begin{aligned}
Q &= \prod_{b\in\mathcal{B}} b \\
&\equiv \prod_{i=1}^{p-1} i^{\frac{q-1}{2}} \quad \bmod p \qquad (21.2)\\
&\equiv (p-1)!^{\frac{q-1}{2}} \bmod p,
\end{aligned}
$$

and

$$
\begin{aligned}
Q &\equiv \prod_{j=1}^{\frac{q-1}{2}} j^{p-1} \qquad \bmod q \qquad (21.3)\\
&\equiv \left(\left(\frac{q-1}{2}\right)!\right)^{p-1} \bmod q.
\end{aligned}
$$

Claim 21.1.

$$\left(\frac{q}{p}\right) R \equiv Q \bmod pq.$$

Proof (of Claim 21.1). For any $1 \leqslant a \leqslant \frac{pq-1}{2}$ with $\gcd(a, pq) = 1$, precisely one of following two must happen:

(i) $a \equiv i \bmod p$ for some $1 \leqslant i \leqslant p-1$ and $a \equiv j \bmod q$ for some $1 \leqslant j \leqslant \frac{q-1}{2}$;

(ii) $a \equiv i \bmod p$ for some $1 \leqslant i \leqslant p-1$ and $a \equiv j \bmod q$ for some $\frac{q+1}{2} \leqslant j \leqslant q-1$.

The second case (ii) is equivalent to

(ii') $a \equiv -i \bmod p$ for some $1 \leqslant i \leqslant p-1$ and $a \equiv -j \bmod q$ for some $1 \leqslant j \leqslant \frac{q-1}{2}$.

In the first case (i), $a \equiv b \bmod pq$ for a unique $b \in \mathcal{B}$ and in the second case (ii'), $a \equiv -b \bmod pq$ for a unique $b \in \mathcal{B}$ by Chinese remainder theorem. Thus

$$
\begin{aligned}
R &= \prod_{a\in\mathcal{A}} a \\
&\equiv \pm \prod_{b\in\mathcal{B}} b \bmod pq \\
&\equiv \pm Q \qquad \bmod pq.
\end{aligned}
$$

But we knew already $\left(\frac{q}{p}\right) R \equiv (p-1)!^{\frac{q-1}{2}} \equiv Q \bmod p$. Further by p is an odd prime, this implies[1] the sign ± equals $\left(\frac{q}{p}\right)$. Hence the Claim 21.1. □

Now let $\mathcal{C}$ be the set of $1 \leqslant c \leqslant pq-1$ with $\gcd(c, pq) = 1$ such that

$$
\begin{aligned}
&c \equiv i \bmod p \text{ for some } 1 \leqslant i \leqslant \frac{p-1}{2}, \text{ and} \\
&c \equiv j \bmod q \text{ for some } 1 \leqslant j \leqslant q-1.
\end{aligned}
$$

Set $P = \prod_{c\in\mathcal{C}} c$, where

$$\mathcal{C} = \left\{1 \leqslant c \leqslant pq-1 : c \equiv i \bmod p \text{ for } 1 \leqslant i \leqslant \frac{p-1}{2} \text{ and } c \equiv j \bmod q \text{ for } 1 \leqslant j \leqslant q-1\right\}.$$

[1] First $R \equiv \pm Q \bmod pq \implies R \equiv \pm Q \bmod p$ since we can reduce the modulus. Then together with $\left(\frac{q}{p}\right) R \equiv Q \bmod p$, we have $\left(\frac{q}{p}\right) R \equiv \pm R \bmod p$. The fact that p is an odd prime will force the congruence to become equality given that $\left(\frac{q}{p}\right)$ can only be ± 1.

By a similar argument to what we have done to $\mathcal{B}$ and $Q = \prod_{b\in\mathcal{B}} b$, we get

$$P \equiv \left(\left(\frac{p-1}{2}\right)!\right)^{q-1} \mod p, \text{ and} \tag{21.4}$$

$$P \equiv (q-1)!^{\frac{p-1}{2}} \mod q. \tag{21.5}$$

Repeat the argument in the proof of Claim 21.1 with switched roles of p and q for P, we can claim

Claim 21.2.

$$\left(\frac{p}{q}\right) R \equiv P \bmod pq.$$

Claim 21.3.

$$Q \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} P \bmod pq.$$

Proof (of Claim 21.3). It suffices to show the congruence holds modulo p and modulo q. First off,

$$\begin{aligned}(p-1)! &= 1\cdot 2\cdot\dots\cdot\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\cdot\dots\cdot(p-2)(p-1)\\ &= 1\cdot 2\cdot\dots\cdot\left(\frac{p-1}{2}\right)\left(p-\frac{p-1}{2}\right)\cdot\dots\cdot(p-2)(p-1)\\ &\equiv \left(\left(\frac{p-1}{2}\right)!\right)^2(-1)^{\frac{p-1}{2}} \bmod p.\end{aligned}$$

Plug this in to Equation (21.2) and raise it to the $\left(\frac{q-1}{2}\right)$-th power, further we get

$$\begin{aligned}Q &\equiv \left(\left(\frac{p-1}{2}\right)!\right)^{q-1}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \bmod p\\ &\equiv P(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \bmod p. && \text{(by Equation (21.4))}\end{aligned}$$

Similarly,

$$(q-1)! \equiv \left(\left(\frac{q-1}{2}\right)!\right)^2(-1)^{\frac{q-1}{2}} \bmod q.$$

Plug it into Equation (21.3) and use Equation (21.5), then

$$\begin{aligned}P &\equiv (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} Q \bmod q \iff\\ Q &\equiv (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} P \bmod q.\end{aligned}$$

This proves Claim 21.3. □

Finally, putting Claims 21.1, 21.2 and 21.3 together, we have

$$\begin{aligned}\left(\frac{q}{p}\right) R &\equiv Q && \bmod pq && \text{(by Claim 21.1)}\\ &\equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} P && \bmod pq && \text{(by Claim 21.3)}\\ &\equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) R && \bmod pq && \text{(by Claim 21.2)}\end{aligned}$$

Since $\gcd(R, pq) = 1$, we can cancel R on both sides to get

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \bmod pq.$$

All terms in the above congruence are ± 1 and pq is odd and $pq > 2$, therefore this forces the congruence to be an equality. We completed the proof of quadratic reciprocity. Phew![2] □

Exercise.

21.1. Let $n \in \mathbb{Z}$, $n > 1$. Show that $2^n - 1 \nmid 3^n - 1$.

21.2. Let p be a prime with $p \neq 2, 3, 5, 11, 17$. Show there exist three different quadratic residues modulo p, denoted r_1, r_2, r_3, such that $r_1 + r_2 + r_3 \equiv 0 \bmod p$.

21.3. Let $p = 2k+1$ be a prime, where $k \in \mathbb{Z}$, $k > 0$. If $p \equiv 7 \bmod 8$, then $\displaystyle\sum_{i=1}^{k} i \left(\frac{i}{p}\right) = 0$, where $\left(\dfrac{i}{p}\right)$ is the usual Legendre symbol. (*Hint*: Try computing $\displaystyle\sum_{i=1}^{p-1} i \left(\frac{i}{p}\right)$ in two different ways.)

[2] The fact that the proof of quadratic reciprocity without the vocabulary of modern algebra ran page after page because of our elementary exposition, indirectly says how powerful the language of abstract algebra is.

LECTURE 22

Day Twenty-Two

— 10.03.2017

Arithmetic functions

DEFINITION 22.1. An **arithmetic function** is a function valued in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, where the domain of the function is the set of positive integers $\mathbb{Z}_{\geqslant 1}$.

EXAMPLE 22.2. The Euler φ-function $\varphi(n)$, counts the number of integers $1 \leqslant a \leqslant n$ such that $\gcd(a, n) = 1$.

EXAMPLE 22.3. The number of divisors function $\nu(n)$, counts the number of positive divisors of n, i.e.,

$$\nu(n) = \sum_{\substack{d \mid n \\ d > 0}} 1$$

for $n \in \mathbb{Z}$, $n > 0$. For example, $\nu(p) = 2$ for any prime p. It is also easy to check $\nu(6) = 4$.

EXAMPLE 22.4. The sum of divisors function $\sigma(n)$, sums up all positive divisors of n, i.e.,

$$\sigma(n) = \sum_{\substack{d \mid n \\ d > 0}} d$$

for $n \in \mathbb{Z}$, $n > 0$. For example, $\sigma(p) = 1+p$ for any prime p. Another example $\sigma(6) = 1+2+3+6 = 12$.

DEFINITION 22.5. An arithmetic function f is **multiplicative** if $f(mn) = f(m)f(n)$ for $m, n \in \mathbb{Z}$, $m, n > 0$ when $\gcd(m, n) = 1$. f is **completely multiplicative** if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}$, $m, n > 0$.

EXAMPLE 22.6. $\varphi(n)$ is multiplicative (See Proposition 13.3) but it is not completely multiplicative, e.g., $\varphi(4) = 2 \neq 1 = \varphi(2)\varphi(2)$.

EXAMPLE 22.7. Fix a prime p. Define an arithmetic function $\chi(n)$ by

$$\chi(n) = \begin{cases} 0 & \text{if } p \mid n, \\ \left(\frac{n}{p}\right) & \text{if } p \nmid n. \end{cases}$$

for $n \in \mathbb{Z}$, $n > 0$. This function is called **Dirichlet character**. Show the Dirichlet character $\chi(n)$ is completely multiplicative.

PROOF. If a prime $p \mid mn$ for $m, n \in \mathbb{Z}$, $m, n > 0$, then $p \mid m$ or $p \mid n$. $\chi(mn) = 0$ since $p \mid mn$. On the other hand, $\chi(m) = 0$ or $\chi(n) = 0$. Therefore $\chi(mn) = \chi(m)\chi(n)$ if $p \mid mn$.

If $p \nmid mn$, then $p \nmid m$ and $p \nmid n$.

$$\begin{aligned} \chi(mn) &= \left(\frac{mn}{p}\right) \\ &= \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \\ &= \chi(m)\chi(n). \end{aligned}$$

The second equality is due to Proposition 19.1 of Legendre symbol. □

Remark 22.8. If f is a multiplicative function, then to compute it, it suffices to know its value on prime powers. If $n \in \mathbb{Z}$, $n > 0$, consider its prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i's are distinct primes, $e_i \in \mathbb{Z}$, $e_i \geqslant 1$ for each $1 \leqslant i \leqslant k$ with $k \in \mathbb{Z}$, $k > 0$. Then

$$f(n) = f(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = f(p_1^{e_1}) f(p_2^{e_2}) \cdots f(p_k^{e_k}).$$

Example 22.9. We saw in Lemma 13.6 that for any prime p and $e \in \mathbb{Z}$, $e \geqslant 1$, for the prime power p^e, we have

$$\varphi(p^e) = (p-1)p^{e-1}.$$

Hence $\varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = (p_1 - 1)p^{e_1 - 1}(p_2 - 1)p^{e_2 - 1} \cdots (p_k - 1)p^{e_k - 1}$, where p_i's are distinct primes and $e_i \in \mathbb{Z}$, $e_i \geqslant 1$. In this way, Theorem 13.5 is immediate.

Theorem 22.10. *Let f be an arithmetic function. Define an arithmetic function F by*

$$F(n) = \sum_{\substack{d \mid n \\ d > 0}} f(d)$$

for any $n \in \mathbb{Z}$, $n > 0$. If f is multiplicative, then F is also multiplicative.

We state a lemma first.

Lemma 22.11. *Let $m, n \in \mathbb{Z}$, $m, n > 0$ with $\gcd(m, n) = 1$. Then for any $d \mid mn$, $d > 0$, there are* ***unique*** *$d_1 \mid m$ and $d_2 \mid n$, $d_1, d_2 > 0$ such that $d = d_1 d_2$. Moreover, if $d_1 \mid m$ and $d_2 \mid n$ with $d_1, d_2 > 0$, then $\gcd(d_1, d_2) = 1$ and $d_1 d_2 \mid mn$.*

Proof (of Lemma 22.11). This is a homework question. See [**Str01**, §3.1, Problem 8]. ■

Proof (of Theorem 22.10). Let $m, n \in \mathbb{Z}$, $m, n > 0$ with $\gcd(m, n) = 1$. Then

$$F(mn) = \sum_{\substack{d \mid mn \\ d > 0}} f(d).$$

By Lemma 22.11, for any $d \mid mn$, d factors uniquely as $d = d_1 d_2$ with $d_1 \mid m$, $d_2 \mid n$, $d_1, d_2 > 0$ and $\gcd(d_1, d_2) = 1$. Conversely, such d_1, d_2 pair gives a $d = d_1 d_2$ such that $d \mid mn$.

Therefore,

$$\begin{aligned}
\sum_{\substack{d \mid mn \\ d > 0}} f(d) &= \sum_{\substack{d_1 \mid m \\ d_2 \mid n \\ d_1, d_2 > 0}} f(d_1 d_2) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n \\ d_1, d_2 > 0}} f(d_1) f(d_2) \qquad \text{(by multiplicativity of } f\text{)} \\
&= \sum_{\substack{d_1 \mid m \\ d_1 > 0}} f(d_1) \sum_{\substack{d_2 \mid n \\ d_2 > 0}} f(d_2) \\
&= F(m)F(n).
\end{aligned}$$

□

Example 22.12. Consider the sum of number of divisors functions $\nu(n) = \sum_{\substack{d \mid n \\ d > 0}} 1$.

The constant function $f(n) = 1$ is (completely) multiplicative for all $n \in \mathbb{Z}$, $n > 0$. Then $\nu(n)$ is also multiplicative by Theorem 22.10. For any prime p and $e \in \mathbb{Z}$, $e \geqslant 0$, $\nu(p^e) = 1 + e$ since $d \mid p^e \iff d = p^f$ for some $0 \leqslant f \leqslant e$, $f \in \mathbb{Z}$.

Thus if $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are nonnegative integers, $k \in \mathbb{Z}$, $k > 0$, then

$$\nu(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \prod_{i=1}^{k} (1 + e_i).$$

This is an application of fundamental theorem of arithmetic.

Example 22.13. The sum of divisors function $\sigma(n) = \sum_{\substack{d \mid n \\ d > 0}} d$ is multiplicative since identify function $f(n) = n$ is multiplicative for all $n \in \mathbb{Z}$, $n > 0$. Let p be a prime and let $e \in \mathbb{Z}$, $e \geqslant 1$. Then

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.$$

Note this also holds when $e = 0$. If $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are nonnegative integers, $k \in \mathbb{Z}$, $k > 0$, then

$$\sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

Remark 22.14. If f is completely multiplicative, we do not necessarily have $F(n) = \sum_{\substack{d \mid n \\ d > 0}} f(d)$ is also completely multiplicative, e.g., $f(n) = 1$ is completely multiplicative but $\nu(n) = \sum_{\substack{d \mid n \\ d > 0}} 1$ is not since $\nu(4) = 3 \neq 4 = \nu(2)\nu(2)$. (Or use another counter example $\sigma(4) = 7 \neq 9 = \sigma(2)\sigma(2)$. Note $f(n) = n$ is completely multiplicative in $\sigma(n) = \sum_{\substack{d \mid n \\ d > 0}} d$.)

Exercise.

22.1. Show $\nu(n) \leqslant 2\sqrt{n}$. (*Hint*: Cut numbers 1 through n at the point $\sqrt{n}$ and count divisors of n from both sides.)

22.2. Show $\varphi(n)\nu(n) \geqslant n$.

22.3. Let $n \in \mathbb{Z}$ with $n > 0$ be a given positive integer. Find the number of integer solutions of

$$\frac{1}{n} = \frac{1}{x} + \frac{1}{y} \text{ with } x, y > 0 \text{ and } x \neq y.$$

22.4. Find all positive integers n such that $\nu(n) = \varphi(n)$. (*Hint*: All such n's are $n = 1$, 3, 8, 10, 18, 24, and 30.)

22.5. Let p, q be primes and let $a, b \in \mathbb{Z}$, $a, b > 0$ with $p^a > q^b$. If $p^a \mid \sigma(p^a)\sigma(q^b)$, then $p^a = \sigma(q^b)$.

22.6. Solve $\varphi(xy) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathbb{Z}$, $x, y > 0$.

22.7. Show that there are infinitely many odd integers n such that $\sigma(n) > 2n$. (*Hint*: 945 is the smallest such positive n.)

LECTURE 23

Day Twenty-Three

— 13.03.2017

Recall from last time, the Euler φ-function satisfies

- the Euler φ-function is multiplicative, i.e., if $m, n \in \mathbb{Z}$, $m, n > 0$ with $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$;
- if p is a prime and $e \in \mathbb{Z}$ with $e \geqslant 1$, then $\varphi(p^e) = (p-1)p^{e-1}$;
- if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with p_i's distinct primes and e_i's positive integers for $1 \leqslant i \leqslant k$, $k \in \mathbb{Z}$, $k > 0$, then $\varphi(n) = \prod_{i=1}^{k}(p_i - 1)p_i^{e_i - 1}$.

Example 23.1. Find <u>all</u> positive integers n such that $\varphi(n) = 42.$[1]

Solution. First, note that $42 = 2 \cdot 3 \cdot 7$. Start with the largest divisor 7. Since 7 is a prime divisor of $\varphi(n)$, consider the prime factorization of n,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i's are distinct primes, and $e_i \geqslant 1$ for $1 \leqslant i \leqslant k$, $k \in \mathbb{Z}$, $k > 0$. By the formula

$$\varphi(n) = \prod_{i=1}^{k}(p_i - 1)p_i^{e_i - 1},$$

we have either $7 \mid p_i - 1$ or $7 \mid p_i^{e_i - 1}$.

(i) If $7 \mid p_i - 1$, note that $p_i - 1$ is bounded by 42 so write down all primes that are smaller than 43 and that are also multiples of 7 plus 1. There are only two possible primes, namely $29, 43$.
   (a) If $p_i = 29$, now write $n = 29m$ with $\gcd(29, m) = 1$, $m \in \mathbb{Z}$, $m > 0$. We can rewrite $\varphi(n) = \varphi(29)\varphi(m) = (29-1)\varphi(m)$, by Euler φ-function being multiplicative. It is easy to see that $28\varphi(m) = 42$ has no integer solutions.
   (b) If $p_i = 43$, again by $\varphi(n) = \varphi(43)\varphi(m) = (43-1)\varphi(m)$, we have $\varphi(m) = 1$. It has two solutions $m = 1, 2$. So $n = 43$ or 86.

(ii) If $7 \mid p_i^{e_i - 1}$, note that $7^{e_i - 1}$ is also bounded by 42, so $e_i \leqslant 2$. At the same time $e_i \geqslant 2$ since the power of 7 survived in the formula of $\varphi(n)$. By a similar argument we have $\varphi(m) = 1$. $m = 1, 2$. The possible n in this case is 49 or 98.

In conclusion, $\varphi(n) = 42 \iff n = 43, 86, 49$ or 98. □

Recall from last lecture, if f is a multiplicative arithmetic function, then $F(n) = \sum_{\substack{d \mid n \\ d > 0}} f(d)$ is also a multiplicative arithmetic function. In particular, $F(n) = \sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = n$ is multiplicative where $f(n) = \varphi(n)$. $\sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = n$ is called **Gauss's identity**.

Theorem 23.2 (Gauss's theorem on divisor sum). *For any $n \in \mathbb{Z}$, $n > 0$, we have $n = \sum_{\substack{d \mid n \\ d > 0}} \varphi(d)$.*

Proof. For a positive divisor e of n, let $\mathcal{S}_e = \{1 \leqslant a \leqslant n : \gcd(a, n) = e\}$.

[1] The original example in the lecture was $\varphi(n) = 28$. $n = 29$ or 58 in that case. The one used here is an example from a homework session.

For all $a \in \mathcal{S}_e$, we have $\gcd(\frac{a}{e}, \frac{n}{e}) = 1$ and $1 \leqslant \frac{a}{e} \leqslant \frac{n}{e}$. On the other hand, if $1 \leqslant b \leqslant \frac{n}{e}$ with $\gcd(b, \frac{n}{e}) = 1$, then $1 \leqslant be \leqslant n$ and $\gcd(be, n) = e$. Thus there is a bijection between $\mathcal{S}_e$ and the set $\{1 \leqslant b \leqslant \frac{n}{e} : \gcd(b, \frac{n}{e}) = 1\}$. Therefore

$$|\mathcal{S}_e| = \left|\left\{1 \leqslant b \leqslant \frac{n}{e} : \gcd(b, \frac{n}{e}) = 1\right\}\right| = \varphi\left(\frac{n}{e}\right).$$

Since every $1 \leqslant a \leqslant n$ lies in an $\mathcal{S}_e$ for some $e \mid n$. And these $\mathcal{S}_e$'s are disjoint for different e's, then we have

$$\begin{aligned} n &= |\{1 \leqslant a \leqslant n\}| \\ &= \sum_{\substack{e \mid n \\ e > 0}} |\mathcal{S}_e| \\ &= \sum_{\substack{e \mid n \\ e > 0}} \varphi\left(\frac{n}{e}\right) \\ &= \sum_{\substack{d \mid n \\ d > 0}} \varphi(d), \end{aligned}$$

by setting $d = \frac{n}{e}$, as e ranges over all positive divisors of n, so does $\frac{n}{e}$.[2] □

[2] Administrative announcement: Midterm 2 covers material up to this point.

Day Twenty-Four

— 15.03.2017

Definition 24.1. A positive integer n is called **a perfect number** if $\sigma(n) = 2n$. Equivalently, $\sigma(n) - n = n$, i.e., the sum of all positive divisors other than n (or the sum of all proper divisors of n) equals n.

Example 24.2. Quick examples.

- 6 is a perfect number since $\sigma(6) - 6 = 1 + 2 + 3 = 6$.
- 28 is a perfect number since $\sigma(28) - 28 = 1 + 2 + 4 + 7 + 14 = 28$.
- No prime number p is perfect since $\sigma(p) - p = 1 < p$ for all prime p.

Lemma 24.3. *Let a be a positive integer. If $2^a - 1$ is prime, then a is prime.*

Proof. We prove the lemma by the contrapositive. If a is not prime, then a is composite. Hence we can write $a = bc$ with $b, c \in \mathbb{Z}$, $1 < b < a, 1 < c < a$. Then we have

$$\begin{aligned} 2^a - 1 &= 2^{bc} - 1 \\ &= (2^b - 1)(2^{bc-b} + 2^{bc-2b} + \cdots + 2^b + 1). \end{aligned}$$

Since $b > 1$, $2^b - 1 > 2^1 - 1 = 1$. Since $c > 1$, $2^{bc-b} + 2^{bc-2b} + \cdots + 2^b + 1 > 1$. ($c$ determines how many terms are in the sum.)

Then $2^a - 1$ is composite. □

Theorem 24.4. *Let $n \in \mathbb{Z}$, $n > 0$ be even. n is a perfect number if and only if $n = 2^{p-1}(2^p - 1)$ with p prime and $2^p - 1$ a Mersenne prime.*

Proof. ($\Leftarrow$) (Euclid) Assume $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ a Mersenne prime. Since $2^p - 1$ is odd, $\gcd(2^{p-1}, 2^p - 1) = 1$. By multiplicativity of σ, we have

$$\begin{aligned} \sigma(n) &= \sigma\big(2^{p-1}(2^p - 1)\big) \\ &= \sigma(2^{p-1})\sigma(2^p - 1) \\ &= \left(\sum_{i=0}^{p-1} 2^i\right)(1 + 2^p - 1) \qquad \text{(by $2^p - 1$ is prime)} \\ &= \frac{2^p - 1}{2 - 1} \cdot 2^p \\ &= 2 \cdot 2^{p-1}(2^p - 1) \\ &= 2n. \end{aligned}$$

($\Rightarrow$) (Euler) Now assume that n is an even perfect number. We can write $n = 2^a m$ with $2 \nmid m$ and $a \in \mathbb{Z}$, $a \geqslant 1$. Since n is perfect, and σ is multiplicative,

$$\begin{aligned} \sigma(n) &= \sigma(2^a m) \\ &= \sigma(2^a)\sigma(m) \\ &= \frac{2^{a+1} - 1}{2 - 1}\sigma(m) \\ &= (2^{a+1} - 1)\sigma(m). \end{aligned}$$

On the other hand, by n a perfect number, $\sigma(n) = 2n = 2 \cdot 2^a m$. So $2^{a+1}m = (2^{a+1} - 1)\sigma(m)$. Note $\gcd(2^{a+1}, 2^{a+1} - 1) = 1$ since two consecutive positive integers are coprime. Therefore $2^{a+1} \mid \sigma(m)$.

Write $\sigma(m) = 2^{a+1}k$ with $k \in \mathbb{Z}$, $k > 0$. Then $2^{a+1}m = (2^{a+1} - 1)2^{a+1}k \implies m = (2^{a+1} - 1)k$. We can show $k = 1$. Otherwise, if $1 < k < m$ and $k \mid m$, then

$$\begin{aligned}\sigma(m) &\geqslant 1 + k + m \\ &= 1 + k + (2^{a+1} - 1)k \\ &= 1 + \sigma(m),\end{aligned}$$

a contradiction. Substitute $k = 1$ into m, then we have $m = 2^{a+1} - 1$.

We now show $2^{a+1} - 1$ is prime, then by Lemma 24.3, $a + 1$ is prime and we are done. Indeed, we saw that $\sigma(m) = 2^{a+1}k = \sigma(2^{a+1} - 1) = 1 + (2^{a+1} - 1)$, since $k = 1$, i.e., $2^{a+1} - 1$ has no other positive divisors than 1 and itself. Hence $2^{a+1} - 1$ is prime. Take $p = a + 1$ we proved the ($\Rightarrow$) direction. □

We stated earlier in Conjecture 16.1 that there are infinitely many Mersenne primes. By Theorem 24.4, Conjecture 16.1 is equivalent to

Conjecture 24.5. *There are infinitely many even perfect numbers.*

Another conjecture about perfect number is

Conjecture 24.6. *There are no odd perfect numbers.*

LECTURE 25

Day Twenty-Five

— 17.03.2017

In Lecture 22, we saw in Theorem 22.10 that given an arithmetic function f, we can build an new arithmetic function $F(n) = \sum_{\substack{d \mid n \\ d > 0}} f(d)$. If f is multiplicative, then so is F.

Question: Can we recover the function f upon which F is built?

First let us try a few examples.

$$\begin{aligned} F(1) &= f(1) && \Longrightarrow \\ f(1) &= F(1). \\ F(2) &= f(1) + f(2) && \Longrightarrow \\ f(2) &= F(2) - F(1). \end{aligned}$$

For any prime p, since $F(p) = f(1) + f(p)$, it implies $f(p) = F(p) - F(1)$. If $n = pq$ with p, q prime and $p \neq q$, then

$$\begin{aligned} F(n) &= F(pq) \\ &= f(1) + f(p) + f(q) + f(pq) \Longrightarrow \\ f(pq) &= F(pq) - \big(F(p) - F(1)\big) - \big(F(q) - F(1)\big) - F(1). \end{aligned}$$

We can continue this. Therefore F does retain all the information about f.

However, is there a clear way of recovering f from F? Yes, recovering f from F is called **Möbius inversion**.

Definition 25.1. The **Möbius function**, denoted μ, is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2 \mid n, \ p \text{ is prime}, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ with } p_1, p_2, \ldots, p_k \text{ distinct primes}, \ k \in \mathbb{Z}_{\geqslant 1}. \end{cases}$$

for any $n \in \mathbb{Z}$, $n > 0$.

Example 25.2. $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(6) = 1$, $\mu(12) = 0$, $\mu(30) = -1$.

Theorem 25.3. *The Möbius function is multiplicative.*

Proof. Let $m, n \in \mathbb{Z}$, $m, n > 0$. If $m = 1$, then $\mu(mn) = \mu(1 \cdot n) = 1 \cdot \mu(n) = \mu(m)\mu(n)$. Similarly, if $n = 1$, $\mu(n)\mu(m) = \mu(mn)$. Either way, $\gcd(1, n) = 1$ or $\gcd(m, 1) = 1$, i.e., with $\gcd(m, n) = 1$ we have $\mu(mn) = \mu(m)\mu(n)$.

Assume $m, n > 1$. If there is a prime p such that $p^2 \mid m$ or $p^2 \mid n$, then $p^2 \mid mn$ and $\mu(mn) = 0 = \mu(m)\mu(n)$.

Now assume $n = p_1 p_2 \cdots p_k$ with $p_1, p_2, \ldots, p_k$ distinct primes and $m = q_1 q_2 \cdots q_\ell$ with $q_1, q_2, \ldots, q_\ell$ distinct primes, $k, \ell \in \mathbb{Z}$, $k, \ell > 0$. If $\gcd(m, n) = 1$, then $p_i \neq q_j$ for any $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant \ell$. Therefore

$$mn = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell$$

is a product of distinct primes. Then $\mu(mn) = (-1)^{\ell + k} = (-1)^{\ell}(-1)^k = \mu(m)\mu(n)$. □

Remark 25.4. μ is not completely multiplicative. For example, $\mu(n \cdot n) = 0 \neq (-1)^{2k} = 1$ for n with $\mu(n) = (-1)^k$.

Then by Theorem 22.10, $F(n)=\sum_{\substack{d\,|\,n\\ d>0}}\mu(d)$ is multiplicative.

Proposition 25.5. *Let $n\in\mathbb{Z}$, $n>0$. Then* $\sum_{\substack{d\,|\,n\\ d>0}}\mu(d)=\begin{cases}1 & \textit{if } n=1,\\ 0 & \textit{otherwise.}\end{cases}$

Proof. If $n=1$, then $\sum_{\substack{d\,|\,n\\ d>0}}\mu(d)=\mu(1)=1$.

Let p be a prime and let $e\in\mathbb{Z}$, $e>0$, then

$$F(p^e)=\sum_{\substack{d\,|\,p^e\\ d>0}}\mu(d)=\sum_{i=1}^{e}\mu(p^i)=1-1+0+0+\cdots+0=0.$$

Then if $n\in\mathbb{Z}$, $n>1$, writing $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ with $p_1,p_2,\ldots,p_k$ distinct primes and $e_1,e_2,\ldots,e_k$ positive integers, then

$$F(n)=\prod_{i=1}^{k}F(p_i^{e_i})=\prod_{i=1}^{k}0,$$

since $F(n)=\sum_{\substack{d\,|\,n\\ d>0}}\mu(d)$ is multiplicative. □

Theorem 25.6 (Möbius inversion). *Let f and g be arithmetic functions. Then $f(n)=\sum_{\substack{d\,|\,n\\ d>0}}g(d)$ if and only if*

$$g(n)=\sum_{\substack{d\,|\,n\\ d>0}}\mu\left(\frac{n}{d}\right)f(d)=\sum_{\substack{d\,|\,n\\ d>0}}\mu(d)f\left(\frac{n}{d}\right).$$

Möbius inversion shows how to recover function g from function f (and vice versa), where μ tracks the sign of $f(d)$ (or of $f\left(\frac{n}{d}\right)$ in the second equality). Before we prove the Möbius inversion, we shall see some immediate consequences of Theorem 25.6.

Example 25.7. Let $n\in\mathbb{Z}$, $n>0$.

- We saw in Theorem 23.2 that $n=\sum_{\substack{d\,|\,n\\ d>0}}\varphi(d)$. Möbius inversion implies

$$\varphi(n)=\sum_{\substack{d\,|\,n\\ d>0}}\mu\left(\frac{n}{d}\right)d.$$

- We saw in Example 22.3 that $\nu(n)=\sum_{\substack{d\,|\,n\\ d>0}}1$. By Möbius inversion, we have

$$1=\sum_{\substack{d\,|\,n\\ d>0}}\mu\left(\frac{n}{d}\right)\nu(d).$$

- We saw in Example 22.4 that $\sigma(n)=\sum_{\substack{d\,|\,n\\ d>0}}d$. By Möbius inversion, we have

$$n=\sum_{\substack{d\,|\,n\\ d>0}}\mu\left(\frac{n}{d}\right)\sigma(d).$$

- By the third example and Gauss's identity, we have

$$\sum_{\substack{d\,|\,n\\ d>0}}\mu\left(\frac{n}{d}\right)\sigma(d)=\sum_{\substack{d\,|\,n\\ d>0}}\varphi(d).$$

Proof (of Möbius inversion). First note that $\sum_{\substack{d \mid n \\ d>0}} \mu\left(\frac{n}{d}\right) f(d) = \sum_{\substack{d \mid n \\ d>0}} \mu(d) f\left(\frac{n}{d}\right)$ holds because as d ranges over all positive divisors of n, so does $\frac{n}{d}$.

($\Rightarrow$) Assume $f(n) = \sum_{\substack{d \mid n \\ d>0}} g(d)$ for $n \in \mathbb{Z}$, $n > 0$. Then

$$\sum_{\substack{d \mid n \\ d>0}} \mu(d) f\left(\frac{n}{d}\right) = \sum_{\substack{d \mid n \\ d>0}} \left(\mu(d) \sum_{\substack{c \mid \frac{n}{d} \\ c>0}} g(c)\right).$$

This double sum is over all pairs d and c with $d \mid n$ and $c \mid \frac{n}{d}$.

This is the same as summing over pairs d and c with $dc \mid n$. (This argument is the bridge between the claims before and after.)

Thus it is the same as summing over pairs d and c with $c \mid n$ and $d \mid \frac{n}{c}$. Therefore

$$\sum_{\substack{d \mid n \\ d>0}} \left(\mu(d) \sum_{\substack{c \mid \frac{n}{d} \\ c>0}} g(c)\right) = \sum_{\substack{c \mid n \\ c>0}} \left(g(c) \sum_{\substack{d \mid \frac{n}{c} \\ d>0}} \mu(d)\right).$$

Note that by Proposition 25.5,

$$\sum_{\substack{d \mid \frac{n}{c} \\ d>0}} \mu(d) = \begin{cases} 1 & \text{if } n = c, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$\sum_{\substack{c \mid n \\ c>0}} \left(g(c) \sum_{\substack{d \mid \frac{n}{c} \\ d>0}} \mu(d)\right) = g(n),$$

which is only term that survives in the sum.

($\Leftarrow$) Now assume $g(n) = \sum_{\substack{d \mid n \\ d>0}} \mu\left(\frac{n}{d}\right) f(d)$. Then

$$\begin{aligned} \sum_{\substack{d \mid n \\ d>0}} g(d) &= \sum_{\substack{d \mid n \\ d>0}} \sum_{\substack{c \mid d \\ c>0}} \mu\left(\frac{d}{c}\right) f(c) \\ &= \sum_{\substack{c \mid n \\ c>0}} f(c) \sum_{\substack{m \mid \frac{n}{c} \\ m>0}} \mu(m) \qquad (25.1) \\ &= f(n). \end{aligned}$$

The second equality of Equation (25.1) is because of a similar argument about pairs $\frac{d}{c}$ and c as above about pairs d and c. Indeed, summing over $\frac{d}{c}$ and c pairs with $d \mid n$ and $c \mid d$ is the same as summing over $d = \frac{d}{c} \cdot c$ with $d \mid n$. Let $m = \frac{d}{c}$, then it is the same as summing over pairs c and m with $c \mid n$ and $m \mid \frac{n}{c}$. The last equality follows since $\frac{n}{c}$ has to be 1 in order for $f(c)$ to survive in the sum according to Proposition 25.5. □

– End of Part 2.

Part 3

March to May, 2017

LECTURE 26

Day Twenty-Six

— 27.03.2017

Primitive roots

The rough goal of our study of primitive roots is to understand the modulo arithmetic of powers. Recall Euler's theorem, Theorem 12.4 says if $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

However, for any a and n as above, we may have $a^e \equiv 1 \bmod n$ for some $0 < e < \varphi(n)$. For example, for any $n > 1$, clearly, $1^1 \equiv 1 \bmod n$.

Definition 26.1. Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a, n) = 1$. The smallest positive integer e such that $a^e \equiv 1 \bmod n$ is called the **order of a modulo n**, written as $\mathrm{ord}_n(a)$.

Remark 26.2. For a and n as in Definition 26.1,

(i) $\mathrm{ord}_n(a)$ exists by Euler's theorem.
(ii) If $b \equiv a \bmod n$, then $\mathrm{ord}_n(b) = \mathrm{ord}_n(a)$.

Example 26.3. Let us find the orders of all integers modulo 9.

Solution. There are $\varphi(9) = 6$ integers that are coprime with 9. They are $1, 2, 4, 5, 7, 8$. It suffices to find the orders of these six integers modulo 9 by (ii) in Remark 26.2. As noted above $\mathrm{ord}_9(1) = 1$.

As for 2,

$$\begin{aligned} 2^1 &= 2 \equiv 2 \bmod 9 \\ 2^2 &= 4 \equiv 4 \bmod 9 \\ 2^3 &= 8 \equiv 8 \bmod 9 \\ 2^4 &= 16 \equiv 7 \bmod 9 \\ 2^5 &= 32 \equiv 5 \bmod 9 \\ 2^6 &= 2^{\varphi(9)} \equiv 1 \bmod 9. \end{aligned}$$

Hence $\mathrm{ord}_9(2) = 6$.

As for 4,

$$\begin{aligned} 4^1 &= 4 \equiv 4 \bmod 9 \\ 4^2 &= 16 \equiv 7 \bmod 9 \\ 4^3 &= 2^6 \equiv 1 \bmod 9. \end{aligned}$$

Hence $\mathrm{ord}_9(4) = 3$.

As for 5,

$$\begin{aligned} 5^1 &= 5 \equiv 5 \bmod 9\\ 5^2 &= 25 \equiv 7 \bmod 9\\ 5^3 &\equiv 7 \times 5 \equiv 8 \bmod 9\\ 5^4 &\equiv 8 \times 5 \equiv 4 \bmod 9\\ 5^5 &\equiv 4 \times 5 \equiv 2 \bmod 9\\ 5^6 &\equiv 2 \times 5 \equiv 1 \bmod 9. \end{aligned}$$

Hence $\mathrm{ord}_9(5) = 6$.

As for 7,

$$\begin{aligned} 7^1 &= 7 \equiv 7 \bmod 9\\ 7^2 &= 49 \equiv 4 \bmod 9\\ 7^3 &\equiv 4 \times 7 \equiv 1 \bmod 9. \end{aligned}$$

Hence $\mathrm{ord}_9(7) = 3$.

As for 8, $8^1 \equiv 8 \bmod 9$, $8^2 = 64 \equiv 1 \bmod 9$. Hence $\mathrm{ord}_9(8) = 2$. □

Proposition 26.4. *Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. A $k \in \mathbb{Z}$, $k \geqslant 1$ satisfies $a^k \equiv 1 \bmod n$ if and only if $\mathrm{ord}_n(a) \mid k$.*

Proof. ($\Leftarrow$) Let $e = \mathrm{ord}_n(a)$. First assume $e \mid k$. Then $k = \ell e$ for some $\ell \in \mathbb{Z}$, $\ell \geqslant 1$. We have $a^k = (a^e)^\ell \equiv 1 \bmod n$ by definition of order of a modulo n.

($\Rightarrow$) Assume $k \in \mathbb{Z}$, $k \geqslant 1$ satisfies $a^k \equiv 1 \bmod n$. By division algorithm,[1] there are unique $q, r \in \mathbb{Z}$ such that

$$k = qe + r \text{ and } 0 \leqslant r < e.$$

Note that $r < e$ and $k > 0$. We have $q \geqslant 0$. Therefore

$$a^k = (a^e)^q a^r \equiv a^r \bmod n.$$

On the other hand, $a^k \equiv 1 \bmod n$ by our assumption, so $a^r \equiv 1 \bmod n$. Since $0 \leqslant r < e$ and e is the smallest positive integer with $a^e \equiv 1 \bmod n$, we must have $r = 0$, i.e., $e \mid k$. □

Corollary 26.5. *$\mathrm{ord}_n(a) \mid \varphi(n)$ for $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$.*

Proof. Take $k = \varphi(n)$ in Proposition 26.4 then the corollary follows. □

Definition 26.6. Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. We say a is a **primitive root modulo** n if $\mathrm{ord}_n(a) = \varphi(n)$.

Example 26.7. We saw in Example 26.3 that 2 and 5 are primitive roots modulo 9.

Question: Do primitive roots always exist? (No.)

Consider modulo 8. We saw in Remark 17.6 that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$. Therefore, any $a \in \mathbb{Z}$ with $\gcd(a, 8) = 1$ has

$$\mathrm{ord}_8(a) = \begin{cases} 1 & \text{if } a \equiv 1 \bmod 8,\\ 2 & \text{if } a \not\equiv 1 \bmod 8. \end{cases}$$

However $\varphi(8) = 4$, meaning $\mathrm{ord}_8(a) < 4$ all the time.

Question: Which positive integers have a primitive root?

To answer this question, we need a slow build-up.

[1] Trick: the "smallest integer" part in the definition of order implies the avenue of the proof might be some inequality involving divisibility. Consider division algorithm.

Proposition 26.8. *Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. Let $k, \ell \in \mathbb{Z}$ such that $k, \ell \geqslant 1$. Then $a^k \equiv a^\ell \bmod n$ if and only if $k \equiv \ell \bmod \mathit{ord}_n(a)$.*

Proof. Let $e = \mathrm{ord}_n(a)$. Without loss of generality, we can assume $k \geqslant \ell$.

($\Leftarrow$) First assume $k \equiv \ell \bmod \mathrm{ord}_n(a)$. Then $k = \ell + qe$ for some $q \in \mathbb{Z}$. Since $k \geqslant \ell$, we have $q \geqslant 0$. Therefore,

$$a^k = (a^e)^q a^\ell \equiv a^\ell \bmod n.$$

($\Rightarrow$) Now assume $a^k \equiv a^\ell \bmod n$. Since $\gcd(a,n) = 1$, there is a unique b such that

$$ab \equiv 1 \bmod n.$$

Since $k \geqslant \ell$, multiply both sides of $a^k \equiv a^\ell \bmod n$ by b^ℓ,

$$\begin{aligned} a^k b^\ell &\equiv a^\ell b^\ell &&\bmod n \\ a^{k-\ell}(ab)^\ell &\equiv (ab)^\ell &&\bmod n \\ a^{k-\ell} &\equiv 1 &&\bmod n. \end{aligned}$$

So we have $\mathrm{ord}_n(a) \mid k - \ell$, i.e., $k \equiv \ell \bmod \mathrm{ord}_n(a)$ by Proposition 26.4. □

Remark 26.9. Proposition 26.8 is the generalization of Proposition 26.4. Indeed, if we substitute $\ell = \mathrm{ord}_n(a)$ in the former then we get $k \equiv 0 \bmod \mathrm{ord}_n(a)$ as in the latter. But note that the proof of Proposition 26.8 actually uses Proposition 26.4, then Proposition 26.4 cannot be treated as a corollary of Proposition 26.8.

LECTURE 27

Day Twenty-Seven

— 29.03.2017

Recall from last time,

PROPOSITION 26.8. *Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. Let $k, \ell \in \mathbb{Z}$ such that $k, \ell \geqslant 1$. Then $a^k \equiv a^\ell \bmod n$ if and only if $k \equiv \ell \bmod ord_n(a)$.*

We will use this proposition to prove the following corollary.

COROLLARY 27.1. *Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. If a is a primitive root modulo n, then any $b \in \mathbb{Z}$ with $\gcd(b,n) = 1$ is congruent modulo n to **precisely** one of*

$$1,\ a,\ a^2,\ \ldots,\ a^{\varphi(n)-1}.$$

PROOF. Since a is a primitive root modulo n, by definition $\operatorname{ord}_n(a) = \varphi(n)$. By Proposition 26.8,

$$a,\ a^2,\ \ldots,\ a^{\varphi(n)-1},\ a^{\varphi(n)}(\equiv 1 \bmod n)$$

are all distinct modulo n. Indeed, if $1 \leqslant k, \ell \leqslant \varphi(n)$ with $a^k \equiv a^\ell \bmod n$, then $k \equiv \ell \bmod \varphi(n)$. But $1 \leqslant k, \ell \leqslant \varphi(n) \implies k = \ell$. We know there are just $\varphi(n)$ distinct congruence classes modulo n consisting of integers coprime with n. We just showed that

$$1,\ a,\ a^2,\ \ldots,\ a^{\varphi(n)-1}$$

define $\varphi(n)$ distinct congruence classes consisting of integers coprime with n. So that is all of them. □

EXAMPLE 27.2. In Example 26.3 we saw 2 is a primitive root modulo 9. So every integer coprime with 9 is congruent modulo 9 to one of

$$1, 2, 2^2, 2^3, 2^4, 2^5.$$

We computed last time

a	$\operatorname{ord}_9(a)$
1	1
2^1	6
2^2	3
2^3	2
2^4	3
2^5	6

and we note that

$$\operatorname{ord}_9(2^2) = 3 = \frac{6}{2} = \frac{\operatorname{ord}_9(2)}{2}$$
$$\operatorname{ord}_9(2^3) = 2 = \frac{6}{3} = \frac{\operatorname{ord}_9(2)}{3}$$
$$\operatorname{ord}_9(2^4) = 3 = \frac{6}{2} = \frac{\operatorname{ord}_9(2)}{2}$$
$$\operatorname{ord}_9(2^5) = 6 = \frac{6}{1} = \frac{\operatorname{ord}_9(2)}{1}.$$

We saw $\operatorname{ord}_9(2^k) = \dfrac{6}{\gcd(6,k)} = \dfrac{\operatorname{ord}_9(2)}{\gcd(\operatorname{ord}_9(2), k)}$ for $2 \leqslant k \leqslant 5$, $k \in \mathbb{Z}$.

Proposition 27.3. *Let $a, n \in \mathbb{Z}$ with $n \geqslant 1$ and $\gcd(a,n) = 1$. For any $k \in \mathbb{Z}$, $k \geqslant 0$, we have*

$$ord_n(a^k) = \frac{ord_n(a)}{\gcd(ord_n(a), k)}.$$

Proof. Let $e = \mathrm{ord}_n(a)$, $f = \mathrm{ord}_n(a^k)$ and $d = \gcd(e,k)$. We want to show $f = \frac{e}{d}$.

Since $d \mid e$ and $d \mid k$, we know

$$(a^k)^{\frac{e}{d}} = (a^{\frac{ke}{d}}) = (a^e)^{\frac{k}{d}} \equiv 1 \bmod n.$$

For this number a^k, $(a^k)^{\frac{e}{d}} \equiv 1 \bmod n$ implies $\mathrm{ord}_n(a^k) \mid \frac{e}{d}$ by Proposition 26.4.

On the other hand, $a^{kf} = (a^k)^f \equiv 1 \bmod n$ since $f = \mathrm{ord}_n(a^k)$. Again by Proposition 26.4, $e \mid kf$ since $e = \mathrm{ord}_n(a)$. Take $d = \gcd(e,k)$, then we have $\frac{e}{d} \mid \left(\frac{k}{d}\right) f$. However $\frac{e}{d}$ and $\frac{k}{d}$ are coprime by Example 4.6. So we must have $\frac{e}{d} \mid f$.

Since $\frac{e}{d} \mid f$ and $f \mid \frac{e}{d}$, both f and $\frac{e}{d}$ are positive integers (by orders are positive, 0 is ruled out), then we have $f = \frac{e}{d}$ as desired. □

Corollary 27.4. *Let $n \in \mathbb{Z}$, $n \geqslant 1$. If there exists a primitive root modulo n, then there are* ***exactly*** *$\varphi(\varphi(n))$ incongruent primitive roots modulo n.*

Proof. Let a be a primitive root modulo n. We saw in Corollary 27.1 the $\varphi(n)$ distinct incongruent classes are described by powers of a,

$$a,\ a^2,\ \ldots,\ a^{\varphi(n)-1},\ a^{\varphi(n)} (\equiv 1 \bmod n).$$

Any potential primitive root is one of these integers that are coprime with n. By Proposition 26.8, for $1 \leqslant k \leqslant \varphi(n)$,

$$\mathrm{ord}_n(a^k) = \varphi(n) \iff \gcd(\varphi(n), k) = 1.$$

There are $\varphi(\varphi(n))$ such k's that are coprime with $\varphi(n)$ for $1 \leqslant k \leqslant \varphi(n)$. □

LECTURE 28

Day Twenty-Eight

— 03.04.2017

Our next goal is to prove the following theorem,

Theorem 28.1. *For any prime p, there exists a primitive root modulo p.*

Proof. The theorem is implied in Corollary 29.2 after we prove Theorem 29.1 in Lecture 29. □

We showed in Proposition 17.5 for an odd prime p and $a \in \mathbb{Z}$, the congruence $x^2 \equiv a \bmod p$ has at most two[1] incongruent solutions modulo p. But we also saw in Remark 17.6 this fails for composite moduli; $x^2 \equiv 1 \bmod 8$ has four incongruent solutions modulo 8.

Theorem 28.2 (Lagrange). *Let p be a prime and let $f(x)$ be a polynomial with integer coefficients,*

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}$ for each $0 \leqslant i \leqslant d$, $d \in \mathbb{Z}$, $d \geqslant 0$. Assume $p \nmid a_d$, the congruence

$$f(x) \equiv 0 \bmod p$$

*has **at most** d incongruent solutions modulo p.*

Proof. If $d = 0$, $a_0 \equiv 0 \bmod p$ with $p \nmid a_0$ has no solutions.

We induct on $d = \deg(f(x))$, $d \geqslant 1$. If $d = 1$, then $f(x) = a_1 x + a_0$.

$$f(x) \equiv 0 \bmod p \iff a_1 x \equiv -a_0 \bmod p,$$

which has a unique solution modulo p by Corollary 10.11 since $p \nmid a_1 \implies \gcd(a_1, p) = 1$. This shows the base case is true.

Assume the result is true for polynomials of degree $d - 1 \geqslant 1$. Let

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0,$$

with $a_i \in \mathbb{Z}$ for each $0 \leqslant i \leqslant d$, $d \in \mathbb{Z}$, $d \geqslant 1$ and $p \nmid a_d$.

If there is no $b \in \mathbb{Z}$ with $f(b) \equiv 0 \bmod p$, then we are done since $f(x) \equiv 0 \bmod p$ has no solutions in that case.

So we can assume there is a $b \in \mathbb{Z}$ with $f(b) \equiv 0 \bmod p$. Note for any $k \in \mathbb{Z}$, $k \geqslant 1$,

$$x^k - b^k = (x - b)(x^{k-1} + x^{k-2}b + \cdots + xb^{k-2} + b^{k-1}).$$

Then notice we can consider instead $f(x) - f(b) \equiv 0 \bmod p$ since $f(b) \equiv 0 \bmod p$ and

$$\begin{aligned} f(x) - f(b) &= (a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0) - \\ &\qquad (a_d b^d + a_{d-1}b^{d-1} + \cdots + a_1 b + a_0) \\ &= a_d(x^d - b^d) + a_{d-1}(x^{d-1} - b^{d-1}) + \cdots + a_1(x - b) + 0 \\ &= (x - b)\underbrace{\left(a_d(x^{d-1} + \cdots + b^{d-1}) + a_{d-1}(x^{d-2} + \cdots + b^{d-2}) + \cdots + a_1\right)}_{\triangleq g(x)} \\ &= (x - b)g(x), \end{aligned}$$

[1] zero or two if $\gcd(a, p) = 1$; one if $p \mid a$.

where $g(x)$ is a degree $d-1$ polynomial with integer coefficients and leading coefficient a_d with $\gcd(a_d, p) = 1$. By our induction hypothesis, $g(x) \equiv 0 \bmod p$ has at most $d-1$ incongruent solutions modulo p. Now

$$\begin{aligned} &\exists\, c \in \mathbb{Z} \text{ such that } f(c) \equiv 0 \mod p \\ &\iff f(c) - f(b) \equiv 0 \bmod p && \text{(by } f(b) \equiv 0 \bmod p\text{)} \\ &\iff (c-b)g(c) \equiv 0 \mod p \\ &\iff c \equiv b \bmod p \text{ or } g(c) \equiv 0 \bmod p. \end{aligned}$$

The last equivalence is due to p is prime. (See Proposition 4.8.) This implies $f(x) \equiv 0 \bmod p$ has at most d incongruent solutions since $g(x) \equiv 0 \bmod p$ has at most $d-1$ incongruent solutions modulo p. The result therefore follows by induction. □

Remark 28.3. Lagrange's theorem parallels what we have been familiar with since grade school, i.e., solutions to polynomials in $\mathbb{R}$ and $\mathbb{Q}$, since $\mathbb{Z}/p\mathbb{Z}$ behaves like a field in a sense as fields $\mathbb{R}, \mathbb{Q}$ do. $((\mathbb{Z}_p, +, \times)$ is a finite field $\mathbb{F}_p$.)

Corollary 28.4. *Let p be a prime and let $d \mid p-1$, $d > 0$. Then the congruence $x^d - 1 \equiv 0 \bmod p$ has* ***exactly*** *d incongruent solutions modulo p.*

Proof. Write $p - 1 = de$ with $e \in \mathbb{Z}$, $e > 0$. Then

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + x^{d(e-2)}) + \cdots + x^d + 1).$$

Lagrange's theorem (Theorem 28.2) implies that

$$x^d - 1 \equiv 0 \bmod p \tag{28.1}$$

has <u>at most</u> d incongruent solutions while

$$x^{d(e-1)} + x^{d(e-2)}) + \cdots + x^d + 1 \equiv 0 \bmod p \tag{28.2}$$

has <u>at most</u> $d(e-1)$ incongruent solutions. By Fermat's little theorem, any $a \in \mathbb{Z}$, $1 \leqslant a \leqslant p$ satisfies

$$a^{p-1} - 1 \equiv 0 \bmod p.$$

Since p is prime, it implies that for any $1 \leqslant a \leqslant p-1$, either $a^d - 1 \equiv 0 \bmod p$ or

$$a^{d(e-1)} + a^{d(e-2)}) + \cdots + a^d + 1 \equiv 0 \bmod p.$$

Since $p - 1 = d + d(e-1)$,[2] we have to max out the number of incongruent solutions of congruences in Equation (28.1) and Equation (28.2) respectively. The first one means nothing but $x^d - 1 \equiv 0 \bmod p$ has exactly d incongruent solutions modulo p. □

[2] $p-1$ is the number of incongruent solutions of congruence $x^{p-1} - 1 \equiv 0 \bmod p$, or the number of integers between 1 and p coprime with p.

Day Twenty-Nine

— 05.04.2017

THEOREM 29.1. *Let p be a prime and let $d \mid p-1$, $d > 0$. There are exactly $\varphi(d)$ incongruent elements with order d modulo p. In particular, for any $d \mid p-1$ with $d > 0$, there is an integer coprime with p that has order d modulo p.*

By Definition 26.6, a primitive root modulo p is an integer a coprime with p such that

$$\operatorname{ord}_p(a) = \varphi(p) = p - 1.$$

Hence the following corollary,

COROLLARY 29.2. *Let p be a prime. There are precisely $\varphi(p-1)$ incongruent primitive roots modulo p. In particular, primitive root modulo p exists.*

EXAMPLE 29.3. Consider the case $p = 19$. Since $19 - 1 = 18$, we have $\varphi(d) = \varphi(1) = 1$ element of order $d = 1$.

PROOF (of Theorem 29.1). For $d \mid p-1$, $d > 0$. Let $N_d = |\{1 \leqslant a \leqslant p-1 : a \in \mathbb{Z}, \operatorname{ord}_p(a) = d\}|$. We want to show $N_d = \varphi(d)$ for every $d \mid p-1$, $d > 0$.

For any $1 \leqslant a \leqslant p-1$, $\operatorname{ord}_p(a) \mid p-1$ by Fermat's little theorem and Proposition 26.4. Thus

$$\sum_{\substack{d \mid p-1 \\ d > 0}} N_d = p - 1.$$

By Gauss's identity (Theorem 23.2)

$$\sum_{\substack{d \mid p-1 \\ d > 0}} \varphi(d) = p - 1.$$

Hence

$$\sum_{\substack{d \mid p-1 \\ d > 0}} N_d = \sum_{\substack{d \mid p-1 \\ d > 0}} \varphi(d). \tag{29.1}$$

For any $d \mid p-1$, $d > 0$, if we can prove $N_d \leqslant \varphi(d)$, Equation (29.1) will force the summands on both sides to be equal, i.e., $N_d = \varphi(d)$.

Fix some $d \mid p-1$, $d > 0$.

(i) If $N_d = 0$, then $N_d < \varphi(d)$.[1]

(ii) If $N_d > 0$, i.e., there is some $1 \leqslant a \leqslant p-1$ such that $\operatorname{ord}_p(a) = d$, by Proposition 26.8 we have the same for powers of a with order d as for primitive roots in Corollary 27.1, that

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

are incongruent modulo p. Also for any $k \in \mathbb{Z}$, $k \geqslant 0$,

$$(a^k)^d \equiv (a^d)^k \equiv 1 \bmod p.$$

[1] We do not know whether such an a with order d exists in the first place. Hence we have to consider $N_d = 0$ case.

Therefore $a, a^2, \dots, a^{d-1}, a^d$ are incongruent solutions to $x^d - 1 \equiv 0 \bmod p$. By the corollary of Lagrange's theorem, Corollary 28.4 implies $x^d - 1 \equiv 0 \bmod p$ has exactly d solutions. Hence any solution to $x^d - 1 \equiv 0 \bmod p$ is congruent modulo p to one of

$$a,\ a^2,\ \dots,\ a^{d-1},\ a^d.$$

In particular, any integer b coprime with p with order d modulo p (b satisfies $x^d - 1 \equiv 0 \bmod p$) is congruent to a^k modulo p for some $1 \leqslant k \leqslant d$. By Proposition 27.3,

$$\begin{aligned} d &= \operatorname{ord}_p(b) \\ &= \operatorname{ord}_p(a^k) = \frac{\operatorname{ord}_p(a)}{\gcd(\operatorname{ord}_p(a), k)} \\ &= \frac{d}{\gcd(d,k)} \iff \gcd(d,k) = 1. \end{aligned}$$

There are $\varphi(d)$ choices for $1 \leqslant k \leqslant d$ with $\gcd(d,k) = 1$. Thus $N_d = \varphi(d)$.

This completes the proof. □

Remark 29.4. In the language of abstract algebra, we proved the group of units $(\mathbb{Z}/p\mathbb{Z})^\times$ in the field $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group. More generally, any finite subgroup of the group of units $\mathbb{F}^\times$ in a field $\mathbb{F}$ is cyclic.

Remark 29.5. Note that the proof gives no indication of how to find primitive roots modulo p. But as for computing all the primitive roots, at least we can trial and error to find the first one, then bootstrap[2] from the one we found.

It is worth noting in the search of primitive roots, if we brute-force sweep all integers starting from 1, say we have the usual set-up, $a, n \in \mathbb{Z}$, $n > 0$ with $\gcd(a, n) = 1$. If a is not a primitive root, then $1 \leqslant a^k < n$ in the target range is not a primitive root either since

$$\begin{aligned} \operatorname{ord}_n(a^k) &= \frac{\operatorname{ord}_n(a)}{\gcd(\operatorname{ord}_n(a), k)} \\ &\leqslant \operatorname{ord}_n(a) \\ &< \varphi(n). && \text{(by } a \text{ is not a primitive root)} \end{aligned}$$

Hence the order of a^k can never be as high as $\varphi(n)$.

Converse to the question we asked, given a prime p whether a primitive root modulo p always exists, E. Artin asked given a primitive root a modulo p, how many such p's are there modulo which a is a primitive root.

Conjecture 29.6 (Artin, 1927). *For any nonsquare integer $a \neq -1$, there are infinitely many primes modulo which a is a primitive root.*

For this open problem, Heath–Brown proved the following theorem,

Theorem 29.7 (Heath–Brown, 1986). *Among all the nonsquare integers $a \neq -1$, there are at most two that do not satisfy Artin's conjecture.*

But Heath–Brown theorem is ineffective to answer Artin's question since Theorem 29.7 does not tell us which two primitive roots a's would fail Conjecture 29.6.

[2] If a is a primitive root modulo p, other primitive roots are congruent to powers of a up to the $\varphi(p)$-th power. Choose $b > 1$ that is coprime with $\varphi(p)$. Compute a^b modulo p, then $c \equiv a^b \bmod p$, $1 \leqslant c < p$ is another primitive root.

LECTURE 30

Day Thirty

— 07.04.2017

Our next goal is to prove the primitive root theorem,

THEOREM 30.1 (Primitive root theorem). *Let $n \in \mathbb{Z}$, $n \geqslant 2$. A primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ with p an odd prime and $k \in \mathbb{Z}$, $k \geqslant 1$.*

Recall from last time that if $n \in \mathbb{Z}$, $n \geqslant 2$ and a is a primitive root modulo n, then any integer coprime with n is congruent to a power a^k modulo n for some $1 \leqslant k \leqslant \varphi(n)$.

EXAMPLE 30.2. Let $n \in \mathbb{Z}$, $n \geqslant 2$ and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Assume that any $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$ is congruent to a^k modulo n for some $k \in \mathbb{Z}$, $k \geqslant 1$. Show a is a primitive root modulo n.

PROOF. By Proposition 26.8, we can convert the congruences of powers of a to congruences of their exponents modulo n. Hence the set of integers $\left\{a^k : k \in \mathbb{Z}, k \geqslant 1\right\}$ defines no more than $\operatorname{ord}_n(a)$ many congruence classes modulo n.

By our assumption, if every b with $\gcd(b, n) = 1$ is congruent to a^k for some $k \in \mathbb{Z}$, $k \geqslant 1$, then $\left\{a^k : k \in \mathbb{Z}, k \geqslant 1\right\}$ defines no less than $\varphi(n)$ many congruence classes modulo n. Thus $\operatorname{ord}_n(a) = \varphi(n)$, i.e., a is a primitive root modulo n. □

COROLLARY 30.3. [1]*Let $a, n \in \mathbb{Z}$, $n \geqslant 2$ and $\gcd(a, n) = 1$. If a is a primitive root modulo n, then a is a primitive root modulo d for any $d \mid n$, $d > 0$.*

COROLLARY 30.4. *Let $k \in \mathbb{Z}$ with $k \geqslant 3$. No primitive root exists modulo 2^k.*

PROOF. Let us assume there is a primitive root a modulo 2^k. Since $k \geqslant 3$, $8 \mid 2^k$. For any $b \in \mathbb{Z}$,

$$\gcd(b, 8) = 1 \iff 2 \nmid b \iff \gcd(b, 2^k) = 1.$$

Our assumption and Example 30.2 imply, for any odd $b \in \mathbb{Z}$, $b \equiv a^m \bmod 2^k$ for some $m \in \mathbb{Z}$, $m \geqslant 1$. Then since $8 \mid 2^k$, by Corollary 30.3, a is a primitive root modulo 8. This contradicts the fact that 8 has no primitive root. □

[1] Proof was not given in the lecture. The reason why it was labeled as a corollary was probably due to the proposition: if a is a primitive root modulo p^k then a is also a primitive root modulo p, whose proof looks like Example 30.2: for any b coprime with p^k, there is an integer $c > 0$ such that $a^c \equiv b \bmod p^k$ hence $a^c \equiv b \bmod p$ by reducing the modulus, i.e., a is also a primitive root of p.

Also apply another proposition: if a is a primitive root modulo n_1n_2, then a is also a primitive root modulo n_1 and n_2. Proof. Assume the contrary, a is not primitive modulo n_1 (or we can consider modulo n_2 similarly), then there exists an integer $0 < c < \varphi(n_1)$ such that $a^c \equiv 1 \bmod n_1$. Let $d = \gcd(n_1, n_2)$. We have $\varphi(n_1n_2) = \varphi(n_1)\varphi(n_2)\frac{d}{\varphi(d)} \geqslant \varphi(n_1)\varphi(n_2) > c\,\varphi(n_2)$, since $\varphi(d) = d\prod_{p|d}(1 - \frac{1}{p})$ or the number of integers 1 through d is definitely greater than or equal to the number of integers up to d that are coprime with d. Then we can raise a to the $c\,\varphi(n_2)$-th power and see if $a^{c\,\varphi(n_2)} \equiv 1 \bmod n_1n_2$ holds. Indeed, by $a^c \equiv 1 \bmod n_1$, if we write $a^c = \ell n_1 + 1$ for some $\ell \in \mathbb{Z}$, then apply binomial theorem to $a^{c\,\varphi(n_2)} = (a^c)^{\varphi(n_2)} = (\ell n_1 + 1)^{\varphi(n_2)}$. We derived a contradiction that a is not a primitive root modulo n_1n_2, since $a^{c\,\varphi(n_2)} \equiv 1 \bmod n_1n_2$ and $c\,\varphi(n_2) < \varphi(n_1n_2)$.

Day Thirty-One

— 10.04.2017

Proposition 31.1. *Let $m, n \in \mathbb{Z}$ with $m, n \geqslant 3$ and $\gcd(m, n) = 1$. Then no primitive root exists modulo mn.*

Proof. Note $\gcd(m, n) = 1$, $m, n > 0$, we have $\varphi(mn) = \varphi(m)\varphi(n)$. Let $d = \gcd\big(\varphi(m), \varphi(n)\big)$ and let $k = \frac{\varphi(mn)}{d} = \frac{\varphi(m)\varphi(n)}{d}$.

Since $m, n \geqslant 3$, we have $2 \mid \varphi(m)$ and $2 \mid \varphi(n)$. So $2 \mid d$. In particular,

$$\begin{aligned} k &= \frac{\varphi(mn)}{d} \\ &< \varphi(mn). \end{aligned}$$

Then for any $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$,

$$\begin{aligned} a^k &= a^{\frac{\varphi(m)\varphi(n)}{d}} \\ &= \left(a^{\varphi(m)}\right)^{\frac{\varphi(n)}{d}} \\ &\equiv 1 \bmod m, \end{aligned}$$

by Euler's theorem. Similarly, $a^k \equiv 1 \bmod n$.

By Chinese remainder theorem, $a^k \equiv 1 \bmod (mn)$ since $\gcd(m, n) = 1$. $k < \varphi(mn)$ implies a is not a primitive root modulo mn. Since a is arbitrary, no primitive root exists modulo mn. □

Corollary 31.2. *Let $n \in \mathbb{Z}$, $n \geqslant 2$. If there is a primitive root modulo n, then $n = 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k \in \mathbb{Z}$, $k \geqslant 1$.*

Proof. We saw in Corollary 30.4 no primitive root exists modulo 2^k if $k \in \mathbb{Z}$, $k \geqslant 3$. If $n = 2^k$ and there is a primitive root modulo n then $k = 1$ or 2.

Now assume n has an odd prime divisor p, i.e., $p \mid n$ with p odd prime. Write $n = p^k m$ with $k \geqslant 1$, $p \nmid m$. Since p is odd and $k \geqslant 1$, $p^k \geqslant 3$ and $\gcd(p^k, m) = 1$. By Proposition 31.1, if there is a primitive root exists modulo $n = p^k m$, then $m < 3$, i.e., $m = 1$ or 2. □

We now prove the converse of Corollary 31.2 is also true, hence we want to complete the proof of Theorem 30.1. This direction is not trivial and requires several steps.

Lemma 31.3. *Let p be a prime and let $a, k \in \mathbb{Z}$ with $k \geqslant 1$ and $p \nmid a$. If a is a primitive root modulo p, then*

$$ord_{p^k}(a) = (p-1)p^m$$

for some $0 \leqslant m \leqslant k - 1$.

Proof. Since $\varphi(p^k) = (p-1)p^{k-1}$. By Corollary 26.5, $\mathrm{ord}_{p^k}(a) \mid \varphi(p^k) = (p-1)p^{k-1}$.

On the other hand, by Definition 26.1, we have

$$\begin{aligned} a^{\mathrm{ord}_{p^k}(a)} &\equiv 1 \bmod p^k \implies \\ a^{\mathrm{ord}_{p^k}(a)} &\equiv 1 \bmod p. \end{aligned}$$

By Proposition 26.4, $\mathrm{ord}_p(a) \mid \mathrm{ord}_{p^k}(a)$. By our assumption, a is a primitive root modulo p, so $\mathrm{ord}_p(a) = \varphi(p) = p-1$. Therefore $p-1 \mid \mathrm{ord}_{p^k}(a)$ and $\mathrm{ord}_{p^k}(a) \mid (p-1)p^{k-1}$. It implies $\mathrm{ord}_{p^k}(a) = (p-1)p^m$ for some $0 \leqslant m \leqslant k-1$. (Consider the prime factorization of $\mathrm{ord}_{p^k}(a)$.) □

Lemma 31.4. *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Assume that a is a primitive root modulo p and that $a^{p-1} \not\equiv 1 \bmod p^2$. Then for any $k \in \mathbb{Z}$ with $k \geqslant 2$, we have*

$$a^{(p-1)p^{k-2}} \not\equiv 1 \bmod p^k$$

and a is also a primitive root modulo p^k.

Proof. By Lemma 31.3, we know that $\mathrm{ord}_{p^k}(a) = (p-1)p^m$ for some $0 \leqslant m \leqslant p-1$ and

$$\begin{aligned}
a \text{ is a primitive root modulo } p^k &\iff m = k-1, \varphi(p^k) = (p-1)p^{k-1}, \text{ in other words,}\\
a \text{ is a not primitive root modulo } p^k &\iff m \leqslant k-2\\
&\iff \mathrm{ord}_{p^k}(a) = (p-1)p^m \text{ with some } 0 \leqslant m \leqslant k-2\\
&\iff a^{(p-1)p^{k-2}} \equiv 1 \bmod p^k,
\end{aligned}$$

since $(p-1)p^m \mid (p-1)p^{k-2}$ when $m \leqslant k-2$.

Assume a is a primitive root modulo p. To prove a is also a primitive root modulo p^k, it suffices to show that

$$a^{(p-1)p^{k-2}} \not\equiv 1 \bmod p^k.$$

We prove this by inducting on $k \geqslant 2$. When $k=2$, this is true by our assumption. Assuming true for $k \geqslant 2$, we prove that it is true for $k+1$. Since $p \nmid a$, by Euler's theorem, we have $a^{(p-1)p^{k-2}} \equiv 1 \bmod p^{k-1}$ (since $\varphi(p^{k-1}) = (p-1)p^{k-2}$). Therefore $a^{(p-1)p^{k-2}} = 1 + bp^{k-1}$ for some $b \in \mathbb{Z}$. Note that by our inductive hypothesis,

$$a^{(p-1)p^{k-2}} \not\equiv 1 \bmod p^k,$$

we have $p \nmid b$. (Otherwise $a^{(p-1)p^{k-2}} = 1 + \ell p \cdot p^{k-1} \equiv 1 \bmod p^k$ for $b = \ell p$ with some $\ell \in \mathbb{Z}$.) Substituting $a^{(p-1)p^{k-2}} = 1 + bp^{k-1}$,

$$\begin{aligned}
a(p-1)p^{k-1} &= \left(a^{(p-1)p^{k-2}}\right)^p\\
&= (1+bp^{k-1})^p\\
&= \sum_{j=0}^{p} \binom{p}{j} b^j p^{j(k-1)}\\
&= 1 + bp^k + \binom{p}{2} b^2 p^{2(k-1)} + \cdots + b^p p^{p(k-1)}.
\end{aligned}$$

Note that if $j \geqslant 3$, $k \geqslant 2$, then $j(k-1) \geqslant k+1$. Therefore

$$\sum_{j=3}^{p} \binom{p}{j} b^j p^{j(k-1)} \equiv 0 \bmod p^{k+1}.$$

Since p is odd, $\frac{p-1}{2}$ is an integer and $\binom{p}{2} bp^{2k-2} = \left(\frac{p-1}{2}\right) bp^{2k-1}$. Since $k \geqslant 2$, $2k-1 \geqslant k+1$. Therefore $\binom{p}{2} bp^{2k-2} \equiv 0 \bmod p^{k+1}$. Hence

$$\begin{aligned}
a^{(p-1)p^{k-1}} &\equiv 1 + bp^k \bmod p^{k+1}\\
&\not\equiv 1 \bmod p^{k+1},
\end{aligned}$$

since $p \nmid b$. By induction we proved the claim. □

Remark 31.5. If we remove p is odd prime in the assumption of Lemma 31.4 so that p could potentially be 2 then the lemma would fail and the inductive proving technique is not effective since when we go from $p^2 = 4$ to $p^3 = 8$, we have seen that 8 does not have primitive root. So we have to rule out $p = 2$.

LECTURE 32

Day Thirty-Two

— 12.04.2017

We continue our effort from last time to prove the primitive root theorem (Theorem 30.1). What Lemma 31.4 does is, since we have known nice properties about p and p^2, Lemma 31.4 will propagate those properties to higher powers of p.

Proposition 32.1. *Let p be an odd prime and let $k \in \mathbb{Z}$, $k \geqslant 1$. Then there exists a primitive root modulo p^k.*

Proof. By Lemma 31.4, it suffices to show that there is an $a \in \mathbb{Z}$ with $p \nmid a$ such that a is a primitive root modulo p and $a^{p-1} \not\equiv 1 \bmod p^2$.

For a prime p, by Corollary 29.2 there is a $b \in \mathbb{Z}$ with $p \nmid b$ and b is a primitive root modulo p.

(i) We can take $a = b$ if $b^{p-1} \not\equiv 1 \bmod p^2$, then we are done.

(ii) Now assume $b^{p-1} \equiv 1 \bmod p^2$. We can choose $a = b + p$. ($a \equiv b \bmod p$ and b is a primitive root modulo p imply a is a primitive root modulo p.) Then

$$\begin{aligned} a^{p-1} &= (b+p)^{p-1} \\ &= \sum_{j=0}^{p-1} \binom{p-1}{j} p^j b^{p-1-j} \\ &= b^{p-1} + (p-1)pb^{p-2} + \sum_{j=2}^{p-1} \binom{p-1}{j} p^j b^{p-1-j} \\ &\equiv 1 - pb^{p-2} \bmod p^2 \qquad\qquad (\text{by } b^{p-1} \equiv 1 \bmod p^2) \\ &\not\equiv 1 \bmod p^2, \end{aligned}$$

since $p \nmid b \implies p^2 \nmid pb^{p-2}$.

We completed the proof. □

Proposition 32.2. *Let p be an odd prime. Then for any $k \in \mathbb{Z}$, $k \geqslant 1$, a primitive root exists modulo $2p^k$.*

Remark 32.3. Given Proposition 32.1, we can expect this proposition to be true simply because $\varphi(2) = 1$. The intuition was it might not be very different when we consider the existence of a primitive root modulo $2p^k$ compared to that modulo p^k.

Proof (of Proposition 32.2). Let $b \in \mathbb{Z}$, $p \nmid b$ be a primitive root modulo p^k, whose existence is guaranteed by Proposition 32.1.

(i) If b is odd, set $a = b$;

(ii) If b is even, set $a = b + p^k$.

Since p^k is odd, in either case, we have a is odd, $p \nmid a$. Hence $\gcd(a, 2p^k) = 1$ and $a \equiv b \bmod p^k$. So a is a primitive root modulo p^k.

By Corollary 26.5, we have

$$\operatorname{ord}_{2p^k}(a) \mid \varphi(2p^k) = (p-1)p^{k-1}.$$

On the other hand,

$$\begin{aligned} & a^{\mathrm{ord}_{2p^k}(a)} \equiv 1 \bmod 2p^k \\ \Longrightarrow\ & a^{\mathrm{ord}_{2p^k}(a)} \equiv 1 \bmod p^k \\ \Longrightarrow\ & \mathrm{ord}_{p^k}(a) \mid \mathrm{ord}_{2p^k}(a), \end{aligned}$$

But $\mathrm{ord}_{p^k}(a) = \varphi(p^k) = (p-1)p^{k-1}$ since a is a primitive root modulo p^k.

So we showed that $\mathrm{ord}_{2p^k}(a) \mid (p-1)p^{k-1}$ and $(p-1)p^{k-1} \mid \mathrm{ord}_{2p^k}(a)$. Therefore,

$$\mathrm{ord}_{2p^k}(a) = (p-1)p^{k-1} = \varphi(2p^k),$$

i.e., a is a primitive root modulo $2p^k$. □

This finally completes the proof of primitive root theorem,

THEOREM 30.1 (Primitive root theorem). *Let $n \in \mathbb{Z}$, $n \geqslant 2$. A primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ with p an odd prime and $k \in \mathbb{Z}$, $k \geqslant 1$.*

REMARK 32.4. The existence of a primitive root a modulo n is useful because it turns questions about the structure of integers coprime with n modulo n into questions about the powers of a, the one particular integer.

As an application, we can prove the generalized Euler's criterion.

DEFINITION 32.5. Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$. For $k \in \mathbb{Z}$, $k \geqslant 1$, we say a is a ***k*-th power residue modulo** n if there is an $x \in \mathbb{Z}$ such that

$$x^k \equiv a \bmod n.$$

EXAMPLE 32.6. Quick examples.

- $5^4 \equiv 4 \bmod 9$. So 4 is a 4th power residue modulo 9.
- -1 is a 3rd power residue modulo 9 since $-1 \equiv 8 \bmod 9$ and $8 = 2^3$.
- $a \in \mathbb{Z}$ with $a \nmid 9$ is a 6th power residue modulo 9 if and only if $a \equiv 1 \bmod 9$. Indeed, if $x \in \mathbb{Z}$ satisfies $x^6 \equiv a \bmod 9$, then $\gcd(x, 9) = 1$ since $\gcd(a, 9) = 1$. By Euler's theorem, $x^6 \equiv 1 \bmod 9$ since $6 = \varphi(9)$.

THEOREM 32.7. *Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$. Let $k \in \mathbb{Z}$ with $k \geqslant 1$. Assume there exists a primitive root modulo n, then a is a k-th power residue modulo n if and only if*

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \bmod n,$$

*where $d = \gcd(\varphi(n), k)$. Moreover, if this is the case, there are **exactly** d incongruent solutions to $x^k \equiv a \bmod n$.*

PROOF. Let r be a primitive root modulo n. Then there is an $\ell \in \mathbb{Z}$, $\ell \geqslant 1$ such that

$$r^\ell \equiv a \bmod n.$$

For any $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$, there is an m, $m \geqslant 1$ such that

$$r^m \equiv x \bmod n. \tag{32.1}$$

Thus

$$\begin{aligned} x^k \equiv a \bmod n \iff & r^{km} \equiv r^\ell \bmod n \\ \iff & km \equiv \ell \mod \varphi(n), \end{aligned} \tag{32.2}$$

since r is a primitive root modulo n and by Proposition 26.8, the exponents of r are congruent modulo the order of r modulo n. It is worth noting, originally, x depends on m chosen in Equation (32.1). What we have done here is turning a problem of solving for x into an equation of m and solving for m itself. The congruence in Equation (32.2) has a solution in m if and only if $d \mid \ell$, where $d = \gcd(\varphi(n), k)$; and if this is the case, there are precisely d incongruent solutions modulo $\varphi(n)$ by Theorem 10.10.

These d incongruent solutions correspond to the d incongruent solutions $x = r^m$ to $x^k \equiv a \bmod n$. (The moral is we convert difficult congruences into linear congruences and solve linear congruences first then convert the solution of linear congruences back to the original difficult congruences.)

Since $r^m \equiv r^{m'} \bmod n$ if and only if $m \equiv m' \bmod \varphi(n)$ by Proposition 26.8, it only remains to show that $d \mid \ell$ if and only if $a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod n$. Indeed,

$$\begin{aligned} d \mid \ell &\iff \ell = ed \text{ for some } e \in \mathbb{Z} \\ &\iff \varphi(n)\ell = \varphi(n)ed \\ &\iff \frac{\varphi(n)}{d}\ell = \varphi(n)e \\ &\iff \frac{\varphi(n)}{d}\ell \equiv 0 \bmod \varphi(n) \\ &\iff r^{\frac{\varphi(n)}{d}\ell} \equiv 1 \bmod n \qquad (32.3)\\ &\iff a^{\frac{\varphi(n)}{d}} \equiv 1 \bmod n, \end{aligned}$$

since $a \equiv r^\ell \bmod n$. Note the equivalent in Equation (32.3), ($\Rightarrow$) direction does not need r to be a primitive root (Euler's theorem), however ($\Leftarrow$) direction requires r to be a primitive root modulo n (Proposition 26.4). □

Remark 32.8. The proof of Theorem 32.7 is just repeatedly applying Proposition 26.8.

Example 32.9 (Example 32.6, continued). Note that $\gcd(\varphi(9), 4) = \gcd(6, 4) = 2$, and $4^{\frac{\varphi(9)}{2}} = 4^{\frac{6}{2}} = 4^3 \equiv 1 \bmod 9$. So 4 is a 4th power residue modulo 9. There are 2 incongruent solutions to $x^4 \equiv 4 \bmod 9$; they are 4 and 5.

Recall Euler's criterion,

Theorem 18.7 (Euler's criterion). *Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then*

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

We can consider Theorem 18.7 as a corollary of Theorem 32.7.

Corollary 32.10. *Let p be an odd prime and let $a \in \mathbb{Z}$, $p \nmid a$. Then a is a quadratic residue modulo p if and only if*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Moreover, if this is the case, there are ***exactly*** *two incongruent solutions to $x^2 \equiv a \bmod p$.*

Proof. Since p is a prime, primitive roots exist modulo p. So we can apply the generalized Euler's criterion (Theorem 32.7) with $k = 2$, in which case, $\gcd(\varphi(n), k) = \gcd(\varphi(p), 2) = 2$. □

Exercise.

32.1. Let p be an odd prime. Solve $x^{p-1} \equiv 1 \bmod p^s$ with $s \in \mathbb{Z}$, $s \geqslant 1$ for all $x \in \mathbb{Z}$.

32.2. Let $a, n \in \mathbb{Z}$ with $n = 2^a + 1$, $a > 1$. Show that n is prime if and only if $3^{\frac{n-1}{2}} \equiv 1 \bmod n$.

LECTURE 33

Day Thirty-Three

— 14.04.2017

Application of primitive roots in cryptography

Recall RSA in Lecture 14. It is asymmetric cryptosystem, i.e., person sending messages and person receiving messages do not share the same information. It is also public in the sense that any one can send messages.

Sometimes it is useful or enough to use a *symmetric* cryptosystem, i.e., where both parties have the same secret information for encrypting and decrypting.

Question: How to generate or share this secret information?

The Diffie-Hellman key exchange is a secure way to share information over an insecure channel.

Remark 33.1. The Advanced Encryption Standard (AES) is a standard cipher that allows one to encrypt and decrypt messages using a secret key, which is an integer both parties have, i.e., different keys give encryptions. Using this, the question becomes how to share a secret integer over an insecure channel.

Remark 33.2. This is often used in conjunction with RSA.

Diffie–Hellman key exchange set-up (Diffie–Hellman, 1976; Williamson, 1974[1]):

- Alice and Bob publicly agree on a large prime p and a primitive root r modulo p;
- Alice chooses a secret positive integer k and sends Bob $1 \leqslant A \leqslant p-1$ with
$$A \equiv r^k \bmod p;$$
- Bob chooses a secret positive integer ℓ and sends Alice $1 \leqslant B \leqslant p-1$ with
$$B \equiv r^\ell \bmod p;$$
- Alice computes B^k modulo p to get
$$r^{k\ell} \equiv B^k \bmod p;$$
- Bob computes A^ℓ modulo p to get
$$r^{\ell k} \equiv A^k \bmod p;$$
- The unique $1 \leqslant s \leqslant p-1$ with $s \equiv r^{k\ell} \bmod p$ is the shared secret key.

Remark 33.3. Why is it secure? Given p, r and A, B, to compute s, we need to find either k or ℓ such that
$$r^k \equiv A \bmod p \text{ or } r^\ell \equiv B \bmod p.$$
But this is a hard problem, called **discrete logarithm problem** in computer science.

A naive algorithm: Compute r^k for each $1 \leqslant k \leqslant p-1$ (or $0 \leqslant k \leqslant p-2$). The run time is about $p-1$ steps. This run time grows exponentially as the #digits of p increases.

A better algorithm is *Baby-Step-Giant-Step algorithm.* It runs in $\mathcal{O}(\sqrt{p-1})$ steps, which is much better than the naive approach. The downside is it needs a lot of storage. The algorithm is based on the observation,

[1] Not declassified until 1997.

Observation. Let r be a primitive root modulo prime p. Let $a \in \mathbb{Z}$ with $p \nmid a$. Then $r^k \equiv a \bmod p$ for some $0 \leqslant k \leqslant p-2$, $k \in \mathbb{Z}$. Let $m = \lceil \sqrt{p-1}\, \rceil$, i.e., the smallest integer $\geqslant \sqrt{p-1}$, we can write $k = im + j$ with $0 \leqslant i, j \leqslant m$. Then we have

$$\begin{aligned} r^k \equiv a \bmod p &\iff r^{im+j} \equiv a \bmod p \\ &\iff r^{i(p-1-m)} r^{im+j} \equiv r^{i(p-1-m)} a \bmod p \\ &\iff r^{i(p-1)} r^j \equiv r^{i(p-1-m)} a \bmod p \\ &\iff r^j \equiv r^{i(p-1-m)} a \bmod p. \qquad (33.1) \end{aligned}$$

The equivalence in Equation (33.1) is due to Fermat's little theorem. The idea of the algorithm is to precompute $r^j \bmod p$ for $0 \leqslant j \leqslant m$ and check if the congruence in Equation (33.1) holds.

Algorithm (Baby-step-giant-step algorithm for discrete logarithm problem):

1. Set $m = \sqrt{p-1}$;
2. Compute $r^j \bmod p$ for each $0 \leqslant j \leqslant m-1$. Store $\big(j, (r^j \bmod p)\big)$;
3. Compute $r^{p-1-m} \bmod p$;
4. Initialize $i = 0$ and $b = a$;
5. Check if $b \equiv r^j \bmod p$ for $0 \leqslant j \leqslant m-1$. If so, return $im + j$; if not,
6. Replace b with $br^{p-1-m} \bmod p$, and i with $i+1$ then go back to the previous step.

Remark 33.4. As for the run time, if we assume step 5 is negligible (which we can), we do m computations in step 2, one computation in step 3, and at most m computations in step 6. Therefore, in total the #steps, $2m + 1 = \mathcal{O}(\sqrt{p-1})$. It is not running in polynomial time but much better than the naive algorithm.

Remark 33.5. There is no known polynomial time (in the #digits of p) algorithm for the discrete logarithm problem. The best known so far is the *number field sieve*[2], which is also the best known algorithm for factoring integers. It is more complicated and requires more theory to describe (Algebraic Number Theory e.g., at least at the level of Math 530).

For example, in 2016, Kleinjung *et al.* [**TKCDaAKLaCPaCS17**] did discrete logarithm computation for a 768 bit prime using number field sieve. The computation took about a year.

[2] Number field, for example, the set of Gauss integers $\{a + ib : a, b \in \mathbb{Z}\}$ with addition and multiplication, where $i^2 = -1$.

LECTURE 34

Day Thirty-Four

— 17.04.2017

Application of primitive roots: Miller–Rabin test (again)

Recall Miller–Rabin test is an efficient way to determine whether or not an integer is a probable prime. See Lecture 15 for the first introduction.

Miller–Rabin test: Given n, an odd positive integer, write $n-1 = 2^k m$ with $k \geqslant 1$ and m odd, $k, m \in \mathbb{Z}$. Choose a random $1 \leqslant a \leqslant n-1$, $a \in \mathbb{Z}$. If $a^m \not\equiv 1 \bmod n$ and $a^{2^r m} \not\equiv -1 \bmod n$ for each $0 \leqslant r \leqslant k-1$, $r \in \mathbb{Z}$, then n is composite. And we say n fails the Miller–Rabin test with this choice of a if $a^m \equiv 1 \bmod n$ or $a^{2^r m} \equiv -1 \bmod n$ for some $0 \leqslant r \leqslant k-1$. But the chances of an odd composite n passing a single Miller–Rabin test are less than a quarter, hence the test is effective because of the following theorem,

Theorem 34.1. *Let $n > 9$ be an odd composite integer. Write $n-1 = 2^k m$ with $k \geqslant 1$ and m odd, $k, m \in \mathbb{Z}$. Let*

$$\mathcal{B} = \left\{ 1 \leqslant a \leqslant n-1 : a^m \equiv 1 \bmod n \text{ or } a^{2^r m} \equiv -1 \bmod n, a \in \mathbb{Z} \text{ for some } 0 \leqslant r \leqslant k-1,\ r \in \mathbb{Z} \right\}.$$

Then $\frac{|\mathcal{B}|}{n-1} < \frac{1}{4}$.

The immediate consequence of Theorem 34.1 is that the chance of an odd composite number $n > 9$ passing 10 (independent) Miller–Rabin tests is less than $\frac{1}{4^{10}} = \frac{1}{1048576} < 0.0001\%$. From computational point of view, primality test and factoring integer are quite different. For example, in `Mathematica`, given $n = 101^{100} + 1$, `PrimeQ[n]` returns `false` instantly. However `FactorInteger[n]` hangs.

Remark 34.2. Miller–Rabin test is a probabilistic primality test. However, assuming some unsolved problems in number theory (generalized Riemann hypothesis, GRH) one can turn the Miller–Rabin test into a deterministic primality test running in polynomial time.

Remark 34.3. In 2002, Agrawal–Kayal–Saxena [**MAaNKaNS04**] developed a deterministic polynomial time primality test without assuming any unsolved problems (such as GRH).

The proof runs for several lectures; it is a long proof.

Proof (of Theorem 34.1). Note any $a \in \mathcal{B}$ must satisfy $\gcd(a, n) = 1$. Indeed, if $e \mid n$ and $e \mid a$, $e \in \mathbb{Z}$, then $e \mid a^m$ and $e \mid a^{2^r m}$ for each $0 \leqslant r \leqslant k-1$. Therefore $e \mid 1$ or $e \mid -1$ since $a \in \mathcal{B}$.

Also since n is composite, $\varphi(n) < n-1$. It suffices to show $\frac{|\mathcal{B}|}{\varphi(n)} \leqslant \frac{1}{4}$. (To be continued.)

Day Thirty-Five

— 19.04.2017

Proof (of Theorem 34.1, continued). Since n is odd, any prime $p \mid n$ is also odd. Let ℓ be the largest positive integer such that $2^\ell \mid p-1$ for each $p \mid n$. Let

$$\mathcal{C} = \left\{1 \leqslant a \leqslant n-1 : \gcd(a,n) = 1 \text{ and } a^{2^{\ell-1}m} \equiv \pm 1 \bmod n\right\}.$$

Claim 35.1. $\mathcal{B} \subseteq \mathcal{C}$.

Remark 35.2 (of Claim 35.1). r in the set $\mathcal{B}$ is a variable, making counting $a \in \mathcal{B}$ difficult. We converted $\mathcal{B}$ to $\mathcal{C}$ and $c \in \mathcal{C}$ is easier to count.

Proof (of Claim 35.1). We can consider two cases of $a \in \mathcal{B}$.

(i) If $a^m \equiv 1 \bmod n$, then

$$\begin{aligned} a^{2^{\ell-1}m} &= (a^m)^{2^{\ell-1}} \\ &\equiv (1)^{2^{\ell-1}} \bmod n \\ &\equiv 1 \qquad \bmod n, \end{aligned}$$

i.e., $a \in \mathcal{C}$.

(ii) Now assume $a^{2^r m} \equiv -1 \bmod n$ for some $0 \leqslant r \leqslant k-1$. Let $p \mid n$ be an odd prime (n is odd) and write[1] $\operatorname{ord}_p(a) = 2^s d$ with $s \geqslant 1$ and $2 \nmid d$. Reducing the modulus,

$$\begin{aligned} a^{2^r m} &\equiv -1 \bmod n \implies \\ a^{2^r m} &\equiv -1 \bmod p, \end{aligned}$$

since $p \mid n$. Therefore $\operatorname{ord}_p(a^{2^r m}) = \operatorname{ord}_p(-1)$. But $\operatorname{ord}_p(-1) = 2$ if p is odd.

On the other hand,

$$\begin{aligned} 2 &= \operatorname{ord}_p(a^{2^r m}) \\ &= \frac{\operatorname{ord}_p(a)}{\gcd(\operatorname{ord}_p(a), 2^r m)} \\ &= \frac{2^s d}{\gcd(2^s d, 2^r m)} \iff 2\gcd(2^s d, 2^r m) = 2^s d. \end{aligned} \tag{35.1}$$

Using the formula for gcd by Proposition 5.5, Equation (35.1) implies[2],

$$2^{1+\min\{s,r\}} = 2^s.$$

Therefore $s = r+1$. $\operatorname{ord}_p(a) = 2^{r+1}d$ with $2 \nmid d$. By Corollary 26.5, $\operatorname{ord}_p(a) \mid p-1$, it implies $2^{r+1} \mid p-1$. By construction of ℓ, we have $\ell \geqslant r+1$. Then

$$\begin{aligned} a^{2^{\ell-1}m} &= (a^{2^r m})^{2^{\ell-1-r}} \\ &\equiv (-1)^{2^{\ell-1-r}} \bmod n \\ &\equiv \pm 1 \qquad \bmod n. \end{aligned}$$

[1] $\gcd(a,n) = 1$ implies $\gcd(a,p) = 1$. p is prime so $\operatorname{ord}_p(a) \mid p-1$ by Corollary 26.5. Note $p-1$ is even if $p > 2$.

[2] We focus on the power of 2.

Note in the last congruence $(-1)^{2^{\ell-1-r}} \equiv -1 \bmod n$ only when $\ell = r+1$. In this case, we have $a \in \mathcal{C}$ as well.

This finishes the verification of the claim, i.e., $\mathcal{B} \subseteq \mathcal{C}$. □

By Claim 35.1, $|\mathcal{B}| \leqslant |\mathcal{C}|$. Hence, it suffices to show $\frac{|\mathcal{C}|}{\varphi(n)} \leqslant \frac{1}{4}$.

Now we want to compute $|\mathcal{C}|$. Consider the prime factorization of n,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j},$$

with p_i odd prime and $e_i \geqslant 1$ for each $1 \leqslant i \leqslant j$, $j \in \mathbb{Z}$, $j > 0$.

Consider the congruence

$$x^{2^{\ell-1}m} \equiv -1 \bmod p_i^{e_i}. \tag{35.2}$$

For each $1 \leqslant i \leqslant j$, there exists a primitive root modulo $p_i^{e_i}$ since p_i is an odd prime by the primitive root theorem (Theorem 30.1). So we can apply the generalized Euler's criterion (Theorem 32.7) to congruence Equation (35.2), i.e., a solution to congruence Equation (35.2) exists if and only if

$$(-1)^{\dfrac{\varphi(p_i^{e_i})}{\gcd\left(\varphi(p_i^{e_i}), 2^{\ell-1}m\right)}} \equiv 1 \bmod p_i^{e_i}, \tag{35.3}$$

and if this is the case, it has exactly $\gcd\left(\varphi(p_i^{e_i}), 2^{\ell-1}m\right)$ many incongruent solutions.

Note if $\frac{\varphi(p_i^{e_i})}{\gcd\left(\varphi(p_i^{e_i}),2^{\ell-1}m\right)}$ is a multiple of 2, then congruence in Equation (35.3) always holds. Since $2^\ell \mid p_i - 1$, we have $2^\ell \mid (p_i-1)p_i^{e_i-1} = \varphi(p_i^{e_i})$. Then

$$\begin{aligned}\gcd\left(\varphi(p_i^{e_i}), 2^{\ell-1}m\right) &= \gcd((p_i-1)p_i^{e_i-1}, 2^{\ell-1}m) \\ &= \gcd(p_i - 1, 2^{\ell-1}m),\end{aligned}$$

since $m \mid n-1$ and $p_i \mid n$ imply $p_i \nmid m$; (Otherwise $p_i \mid m \implies p_i \mid n-1$, and with $p_i \mid n$, it implies $p_i \mid n-(n-1) = 1$, a contradiction.) Also p_i is odd, $p_i \nmid 2$, hence $p_i \nmid 2^{\ell-1}m$.

Further

$$\gcd(p_i - 1, 2^{\ell-1}m) = 2^{\ell-1}\gcd(p_i-1, m),$$

since $2^\ell \mid p_i - 1 \implies 2^{\ell-1} \mid p_i - 1$. Therefore the exponent of (-1) in Equation (35.3),

$$\frac{\varphi(p_i^{e_i})}{\gcd\left(\varphi(p_i^{e_i}), 2^{\ell-1}m\right)} = \frac{(p_i-1)p_i^{e_i-1}}{2^{\ell-1}\gcd(p_i-1,m)} \text{ is divisible by 2,}$$

since $p_i - 1$ in the numerator has ℓ copies of 2 and $\gcd(p_i-1,m)$ in the denominator has no copies of 2. Thus the congruence in Equation (35.3) always holds, i.e., congruence Equation (35.2) has exactly $2^{\ell-1}\gcd(p_i-1,m)$ incongruent solutions by generalized Euler's criterion.

By Chinese remainder theorem, each choice of solution modulo $p_i^{e_i}$ for each $1 \leqslant i \leqslant j$ corresponds to a unique solution modulo $n = \prod_{i=1}^j p_i^{e_i}$ to congruence

$$x^{2^{\ell-1}m} \equiv -1 \bmod n. \tag{35.4}$$

The number of incongruent solutions to congruence Equation (35.4) is

$$\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m).$$

A similar argument can be said about congruence

$$x^{2^{\ell-1}m} \equiv +1 \bmod n. \tag{35.5}$$

There are also

$$\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m)$$

many incongruent solutions to congruence Equation (35.5). So the size of $\mathcal{C}$ is

$$|\mathcal{C}| = 2\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i - 1, m).$$

Since

$$\begin{aligned} \frac{|\mathcal{C}|}{\varphi(n)} &\leqslant \frac{1}{4} \\ \iff \quad \frac{2\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m)}{\prod_{i=1}^{j}(p_i-1)p_i^{e_i-1}} &\leqslant \frac{1}{4} \\ \iff \quad 8\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m) &\leqslant \prod_{i=1}^{j}(p_i-1)p_i^{e_i-1}, \end{aligned}$$

next we need to show

$$8\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m) \leqslant \prod_{i=1}^{j}(p_i-1)p_i^{e_i-1}$$

for all $n > 9$.

Day Thirty-Six

— 21.04.2017

PROOF (of Theorem 34.1, continued). Recall from last time, we want to show

$$8\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m) \leqslant \prod_{i=1}^{j}(p_i-1)p_i^{e_i-1}$$

for all $n > 9$. Assume the contrary, i.e.,

$$8\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m) > \prod_{i=1}^{j}(p_i-1)p_i^{e_i-1}. \tag{36.1}$$

Since $2^\ell \mid p_i - 1$ for each $1 \leqslant i \leqslant j$, $\gcd(p_i-1,m) \mid p_i - 1$ for each $1 \leqslant i \leqslant j$, and $\gcd(p_i-1,m)$ is odd (as m is odd), we have

$$2^\ell \gcd(p_i-1,m) \mid p_i - 1.$$

In particular, $p_i - 1 \geqslant 2^\ell \gcd(p_i-1,m)$. Then the inequality in Equation (36.1) implies

$$\begin{aligned} 8\prod_{i=1}^{j} 2^{\ell-1}\gcd(p_i-1,m) &> \prod_{i=1}^{j}(p_i-1)p_i^{e_i-1} \\ &\geqslant \prod_{i=1}^{j} 2^{\ell}\gcd(p_i-1,m)p_i^{e_i-1} \\ \implies 8 &> \prod_{i=1}^{j} 2p_i^{e_i-1}, \qquad (36.2) \end{aligned}$$

i.e., we must have $j \leqslant 2$.

(i) First assume $j = 2$. We can write $n = p_1^{e_1}p_2^{e_2}$ with p_1, p_2 distinct odd primes, $e_1, e_2 \geqslant 1$, $e_1, e_2 \in \mathbb{Z}$. Plug n into the inequality in Equation (36.2),

$$8 > 4p_1^{e_1-1}p_2^{e_2-1}.$$

It implies $e_1 = e_2 = 1$. Then the inequality in Equation (36.1) becomes

$$2 > \frac{p_1-1}{2^\ell\gcd(p_1-1,m)} \cdot \frac{p_2-1}{2^\ell\gcd(p_2-1,m)}.$$

This means $p_i - 1 = 2^\ell \gcd(p_i-1,m)$ for $i = 1, 2$. Set $d_i = \gcd(p_i-1,m)$. Note $d_i \mid m$, so

$$\begin{aligned} p_1p_2 &= n \\ &= 1 + 2^k m \\ &\equiv 1 \bmod d_i \text{ for } i = 1, 2. \end{aligned}$$

And also $p_i - 1 = 2^\ell d_i$ for $i = 1, 2$ as well, i.e., $p_i \equiv 1 \bmod d_i$. But

$$\begin{cases} p_1 \equiv 1 \bmod d_1 \\ p_1p_2 \equiv 1 \bmod d_1 \end{cases} \implies p_2 \equiv 1 \bmod d_1.$$

Hence $d_1 \mid p_2 - 1$. Also note d_1 is odd, $d_1 \mid p_2 - 1 = 2^\ell d_2 \implies d_1 \mid d_2$.

A symmetric argument says $d_2 \mid d_1$. Therefore, $d_1 = d_2$. Consequently, $p_1 = 1 + 2^\ell d_1 = 1 + 2^\ell d_2 = p_2$, a contradiction.

(ii) Now assume $j = 1$. We write $n = p^e$ with p odd prime and $e \geqslant 2$ (since n is composite). Then the inequality in Equation (36.2) becomes

$$4 > p^{e-1}.$$

With p odd prime and $e \geqslant 2$, this is only possible if $p = 3$ and $e = 2$. Then $n = 3^2 = 9$, a contradiction since $n > 9$ by our assumption.

Finally we completed the proof of Theorem 34.1. □

We will move to our next new topic.

Diophantine equations

A **Diophantine equation** is a polynomial equation in two or more variables that we want to solve for integer solutions.

Example 36.1. Let $a, b, c \in \mathbb{Z}$. We saw in Lecture 7, Proposition 7.1 that the linear Diophantine equation in two variables

$$ax + by = c$$

has solutions in $x, y \in \mathbb{Z}$ if and only if $\gcd(a, b) \mid c$, and if this is the case, we can find all solutions.

Question: What about nonlinear Diophantine equations?

The answer is it depends on the specific settings. However, a useful trick is based on the following observation.

Observation. If a Diophantine equation has solutions in $\mathbb{Z}$, then it has solutions modulo n for any $n \in \mathbb{Z}$, $n \geqslant 1$.

Example 36.2. Consider the equation $3x^2 - y^2 = 1$. If $x, y \in \mathbb{Z}$ exist such that they solve the Diophantine equation, then

$$\begin{aligned} 3x^2 - y^2 &\equiv 1 \bmod 3 \\ -y^2 &\equiv 1 \bmod 3 \\ y^2 &\equiv 2 \bmod 3. \end{aligned}$$

However, 2 is not a quadratic residue modulo 3. Hence no integer solution in y exists.

Remark 36.3. This trick however does not always work for showing nonexistence of solutions!

Example 36.4. Consider the equation $(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$. It has no integer solutions but it has solutions modulo n for any $n \geqslant 1$.

Proof. For $n = 1$, it is trivial since any integer is congruent to 0 modulo 1.[1] We can assume $n \geqslant 2$.

Let $n = \prod_{p \mid n} p^e$ be the prime factorization of n. By Chinese remainder theorem, the congruence equation has a solution modulo n if and only if it has a solution modulo p^e for each $p \mid n$,

$$\begin{aligned} &(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \bmod n \\ \iff &(x^2 - 2)(x^2 - 17)(x^2 - 34) \equiv 0 \bmod p^e. \end{aligned}$$

[1] In computer programming, this fact can be used to set up an integral test, i.e., to test if a variable assumes an integer value, simply check if that value modulo 1 is zero.

It further suffices to show at least one of

$$x^2 \equiv 2 \mod p^e \tag{36.3}$$

$$x^2 \equiv 17 \bmod p^e \tag{36.4}$$

$$x^2 \equiv 34 \bmod p^e \tag{36.5}$$

has a solution. For a prime power p^e with $e \geqslant 1$, $e \in \mathbb{Z}$ and $a \in \mathbb{Z}$ with $p \nmid a$, $x^2 \equiv a \bmod p^e$ is solvable if and only if

$$\begin{cases} a \equiv 1 \bmod 8 & \text{if } p = 2 \text{ and } e \geqslant 3, \\ x^2 \equiv a \bmod p \text{ is solvable} & \text{if } p > 2. \end{cases} \tag{36.6}$$

For details, see [Str01, §4.1, Problem 11].

We can look at three cases.

(i) If $p = 2$, then congruence Equation (36.4) has a solution for $e \geqslant 3$ since $17 \equiv 1 \bmod 8$. When $e = 1$ or 2, quick inspection reveals both $x^2 \equiv 17 \bmod 2$ and $x^2 \equiv 17 \bmod 4$ are solvable.

(ii) If $p = 17$, then $x^2 \equiv 2 \bmod 17$ is solvable by the second supplement to quadratic reciprocity (Theorem 19.2) since $17 \equiv 1 \bmod 8$. Therefore by the equivalence in Equation (36.6), the congruence Equation (36.3) is always solvable when $p = 17$.

(iii) If $p \neq 2$ or 17, then one of $2, 17, 34$ is a quadratic residue modulo p since

$$\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right).$$

Therefore at least one of Equations (36.3), (36.5), (36.5) is solvable. □

Exercise.

36.1. Let $k, m \in \mathbb{Z}$ such that $m^2 + 3 = 2k$. Is it possible to write k as the sum of three squares? (*Hint*: m is odd.)

36.2. Find all positive integers m such that $n^4 + m$ is not a prime for any positive integer n. (*Hint*: $m = 4k^4$, $k \in \mathbb{Z}$ is one candidate.)

36.3. Let $a, b \in \mathbb{Z}$, $a, b > 0$. Show $x^{2a+1} = 2^b \pm 1$ has no integer solution when $x > 1$.

LECTURE 37

Day Thirty-Seven

— 24.04.2017

Consider the Diophantine equation $x^2 + y^2 = z^2$.
It has solutions in $\mathbb{Z}$, for example,

(1) $3^2 + 4^2 = 5^2$.
(2) $1^2 + 0^2 = 1^2$. Or for any $a \in \mathbb{Z}$, we have $a^2 + 0^2 = a^2$.
(3) $(-3)^2 + 4^2 = (-5)^2$.
(4) $6^2 + 8^2 = 10^2$.

Definition 37.1. Positive integers x, y, z satisfying $x^2 + y^2 = z^2$ are called **Pythagorean triple**. We say a Pythagorean triple is **primitive** if $\gcd(x, y, z) = 1$.

Remark 37.2. The name Pythagorean triple comes from the Pythagorean theorem, named after Greek mathematician Pythagoras. But the Pythagorean theorem was known to the Mesopotamian, Indian and Chinese all independently. Even with some indication it was known in ancient Babylon.

Let us understand primitive Pythagorean triples. Understanding primitive Pythagorean triples is enough since if x, y, z is any Pythagorean triple and $d = \gcd(x, y, z)$, then

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \left(\frac{z}{d}\right)^2.$$

And $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ is a primitive triple.

Claim 37.3. one of x, y is even and the other is odd in the primitive Pythagorean triple x, y, z.

Proof. We can consider the cases where both x and y are even or odd.

(i) If $2 \mid x$ and $2 \mid y$, then $2 \mid x^2 + y^2$, i.e., $2 \mid z^2 = x^2 + y^2 \implies 2 \mid z$. x, y, z is not a primitive triple.
(ii) If x and y are both odd, then $x^2 \equiv \pm 1 \bmod 4$ and $y^2 \equiv \pm 1 \bmod 4$. So $x^2 + y^2 \equiv 2 \bmod 4$. But for any $z \in \mathbb{Z}$,

$$z^2 \equiv \begin{cases} 0 \bmod 4 & \text{if } z \text{ is even,} \\ 1 \bmod 4 & \text{if } z \text{ is odd.} \end{cases}$$

We get a contradiction.

Hence the claim. □

From this point on, without loss of generality, we can assume x is odd, y is even and we mainly consider primitive Pythagorean triples.

Theorem 37.4. *x, y, z is a primitive Pythagorean triple with x odd and y even if and only if there are $m, n \in \mathbb{Z}$ with $m > n > 0$, $\gcd(m, n) = 1$, and exactly one of m, n is even, the other is odd such that*

$$x = m^2 - n^2, \ y = 2mn, \ \text{and } z = m^2 + n^2.$$

*In particular, there are **infinitely many** primitive Pythagorean triples.*

Example 37.5. Quick examples.

- If $m = 2$, $n = 1$, then $x = 3$, $y = 4$, $z = 5$ is a primitive Pythagorean triple.
- If $m = 3$, $n = 2$, then $x = 5$, $y = 12$, $z = 13$ is a primitive Pythagorean triple.

- If $m = 4$, $n = 1$, then $x = 15$, $y = 8$, $z = 17$ is a primitive Pythagorean triple.

REMARK 37.6. If we change the above quadratic Diophantine equation $x^2+y^2 = z^2$ into $x^2+y^2 = 3z^2$, then we can show it has no nontrivial solutions. Further by Fermat's last theorem, there are no solutions to $x^n + y^n = z^n$ with nonzero $x, y, z \in \mathbb{Z}$ for any $n \geqslant 3$.

This illustrates the subtlety of Diophantine equations—a small variation can completely change the answer.

PROOF (of Theorem 37.4). ($\Leftarrow$) First let $m, n \in \mathbb{Z}$ with $m > n > 0$, $\gcd(m, n) = 1$, and exactly one of m, n is even. Setting

$$x = m^2 - n^2,\ y = 2mn,\ \text{and}\ z = m^2 + n^2,$$

we check if $x^2 + y^2 = z^2$. Indeed,

$$x^2 + y^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = z^2.$$

Note that $x, y, z > 0$ by $m > n > 0$, x, y, z is a Pythagorean triple. Note also that y is even, x is odd and exactly one of m, n is even by our assumption. We need to check if $\gcd(x, y, z) = 1$.

Let $d = \gcd(x, y, z)$, since x is odd and $d \mid x$, d is also odd. Since $d \mid x$, $d \mid z$, we have $d \mid x+z = 2m^2$ and $d \mid z - x = 2n^2$. $d \mid 2m^2$ and $d \mid 2n^2$ while at the same time, $\gcd(m, n) = 1 \implies \gcd(m^2, n^2) = 1$. Then we know d comes from 2. But d is odd so $d = 1$.

($\Rightarrow$) Now assume x, y, z is a primitive Pythagorean triple with x odd, y even. First notice $\gcd(x, y) = 1$. (Otherwise they share some odd common divisor such that an odd prime $p \mid x$ and $p \mid y$. It further implies $p \mid x^2 + y^2 = z^2$ therefore x, y, z is not a primitive triple.)

Since x, y, z is primitive implies $\gcd(x, y) = 1$, similarly we get $\gcd(y, z) = \gcd(z, x) = 1$. Since x is odd, y is even, z is odd and each of y, $z - x$ and $z + x$ is even, we get

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right), \tag{37.1}$$

where $\frac{z\pm x}{2} \in \mathbb{Z}$.

Let $e = \gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right)$. Then

$$e \left| \frac{z-x}{2} + \frac{z+x}{2} \right. \implies e \mid z,$$
$$e \left| \frac{z-x}{2} - \frac{z+x}{2} \right. \implies e \mid x.$$

But $\gcd(z, x) = 1$. Therefore $e = 1$, i.e., $\left(\frac{z-x}{2}\right)$ and $\left(\frac{z+x}{2}\right)$ are coprime. By fundamental theorem of arithmetic, Equation (37.1) implies that there are $m, n \in \mathbb{Z}$, $m, n > 0$ such that

$$\frac{z+x}{2} = m^2,\ \frac{z-x}{2} = n^2,\ \text{and}\ \frac{y}{2} = mn.$$

Then $x = m^2 - n^2$, $z = m^2 + n^2$ and $y = 2mn$. Since $x > 0$, $x = m^2 - n^2 > 0 \implies m > n > 0$. Further,

$$\gcd\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = \gcd(m^2, n^2) = 1,$$

which implies $\gcd(m, n) = 1$. Finally, since $x = m^2 - n^2$ is odd, exactly one of m, n is even. □

Exercise.

37.1. Solve

$$\begin{cases} x^3 + y^3 + z^3 = 3 \\ x + y + z = 3 \end{cases}$$

for all $x, y, z \in \mathbb{Z}$. (*Hint*: There are four solutions: $(x, y, z) = (1, 1, 1)$, $(-5, 4, 4)$, $(4, -5, 4)$, and $(4, 4, -5)$.)

37.2. Solve $3 \cdot 2^x + 1 = y^2$ for all $x, y \in \mathbb{Z}$. (*Hint*: There are two solutions: $(x, y) = (3, 5)$, $(4, 7)$.)

37.3. Solve $y^2 = 1 + x + x^2 + x^3 + x^4$ for all $x, y \in \mathbb{Z}$. (*Hint*: There are six solutions: $(x, y) = (-1, \pm 1)$, $(0, \pm 1)$, and $(3, \pm 11)$.)

37.4. Solve $x^2 + y^2 + z^2 = x^2 y^2$ for all $x, y, z \in \mathbb{Z}$. (*Hint*: The only integer solutions are $x = y = z = 0$.)

LECTURE 38

Day Thirty-Eight

— 26.04.2017

Recall Theorem 37.4 characterizes solutions to the Diophantine equation

$$x^2 + y^2 = z^2.$$

Question: What are the integer solutions to $x^n + y^n = z^n$ for $n \geqslant 3$?

THEOREM 38.1 (Fermat's last theorem, Wiles and Taylor–Wiles, 1995). *For any $n \in \mathbb{Z}$, $n \geqslant 3$,*

$$x^n + y^n = z^n$$

*has **no** solutions with x, y, z nonzero integers.*

REMARK 38.2. For $n \in \mathbb{Z}$, $n > 0$, if $x, y, z \in \mathbb{Z}$ are nonzero integers such that $x^n + y^n = z^n$, then for any $d \mid n$, $d > 0$, $x^{\frac{n}{d}}, y^{\frac{n}{d}}, z^{\frac{n}{d}}$ are nonzero integers satisfying

$$\left(x^{\frac{n}{d}}\right)^d + \left(y^{\frac{n}{d}}\right)^d = \left(z^{\frac{n}{d}}\right)^d.$$

So to prove there are no solutions when $n \geqslant 3$, it suffices to show Fermat's last theorem holds for $n = 4$ and n odd primes.[1]

The general timeline of the progress towards the proof:

- Germain (1820s) proved that for all odd primes $p < 197$, $x^p + y^p = z^p$ has no solutions with x, y, z coprime with p.
- Lamé in 1847 gave a false proof based on the following ideas:

  Let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ with p a fixed odd prime. In the previous lecture on Pythagorean triples, we looked at $y^2 = (z - x)(z + x)$. If $x^p + y^p = z^p$, $x, y, z \in \mathbb{Z}$ then

  $$\begin{aligned} y^p &= z^p - x^p \\ &= \prod_{i=1}^{p} (z - \zeta^i x) \text{ in } \mathbb{C}. \end{aligned}$$

  Lamé showed that Fermat's last theorem is true if the number ring

  $$\mathbb{Z}[\zeta] = \left\{a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} : a_i \in \mathbb{Z}\right\} \subseteq \mathbb{C}$$

  holds unique factorization of primes, i.e., fundamental theorem of arithmetic holds. But this is false in general (pointed out by Kummer).[2]
- Special case of Faltings (1983) is that $x^p + y^p = z^p$ has finitely many nonzero solutions.
- The proof was finally given by Wiles and Taylor–Wiles in 1995 built upon the work of Frey, Serre and Ribet in the 1980s.

Annals of Mathematics dedicated a special issue to the Wiles proof and it ran over 100 pages. We only prove $n = 4$ case in this course.

Note if x, y, z are nonzero integers such that

$$x^4 + y^4 = z^4 = (z^2)^2,$$

[1] The reduction follows from the fact that for any divisor of n, if $x^d + y^d = z^d$ has no solutions then $x^n + y^n = z^n$ cannot have solutions. For powers of 2, $n = 2^k$, $k \geqslant 2$, it reduces to the case $n = 4$. For other n's, it suffices to ensure $x^p + y^p = z^p$ has no solutions, where $p \mid n$, p an odd prime.

[2] Kummer is one of the "$K3$" after whose names $K3$-surface is named. The other two are Kähler and Kodaira.

then it suffices to prove

THEOREM 38.3. *There are no nontrivial integers solutions to* $x^4 + y^4 = z^2$.

PROOF. We prove by Fermat's infinite descent. Assume otherwise, then replacing x, y, z with their negation if necessary, we can assume $x, y, z > 0$. We can also assume $\gcd(x, y) = 1$.[3]

Now assume there exists a triple $x_1, y_1, z_1 \in \mathbb{Z}$ such that $x_1^4 + y_1^4 = z_1^2$, $x_1, y_1, z_1 > 0$, $\gcd(x_1, y_1) = 1$, and z_1 is the smallest possible. We want to construct another solution x_2, y_2, z_2 with $x_2, y_2, z_2 > 0$, $\gcd(x_2, y_2) = 1$, and $z_2 < z_1$. This will yield a contradiction.

Note that x_1^2, y_1^2, z_1 is a Pythagorean triple. It is also primitive since $\gcd(x_1, y_1) = 1$ implies $\gcd(x_1^2, y_1^2) = 1$.[4] By Claim 37.3 we saw last time exactly one of x_1^2, y_1^2 is even, and swap x_1, y_1 if necessary, we can assume y_1^2 is even, x_1^2 is odd, i.e., x_1 is odd, y_1 is even.

By Theorem 37.4, there are $m, n \in \mathbb{Z}$ with $m > n > 0$, $\gcd(m, n) = 1$, and exactly one of m, n is even such that

$$x_1^2 = m^2 - n^2, \; y_1^2 = 2mn, \; \text{and } z_1 = m^2 + n^2.$$

Then $x_1^2 + n^2 = m^2 \implies x_1, n, m$ is another Pythagorean triple. It is primitive since $\gcd(m, n) = 1$. Since x_1 is odd, by Theorem 37.4 again, n is even, m is odd. Repeat, there are $a, b \in \mathbb{Z}$ with $a > b > 0$, $\gcd(a, b) = 1$ and exactly one of a, b even such that

$$x_1 = a^2 - b^2, \; n = 2ab, \; \text{and } m = a^2 + b^2.$$

Our target is to show that m, a, b are squares. Indeed, we have $y_1^2 = (2n)m$, $\gcd(m, 2n) = 1$ since $\gcd(m, n) = 1$, m is odd. By fundamental theorem of arithmetic, m and $2n$ are squares. Since $2n$ is even and a square, there is a $c \in \mathbb{Z}$ such that $(2c)^2 = 2n$, which implies $n = 2c^2$. $n = 2ab = 2c^2 \implies ab = c^2$. But $\gcd(a, b) = 1$, again by fundamental theorem of arithmetic, a, b are both squares.

We showed that there are $x_2, y_2, z_2 \in \mathbb{Z}$, $x_2^2 = a$, $y_2^2 = b$, and $z_2^2 = m$. Replacing x_2, y_2, z_2 with their negations if necessary, we can assume $x_2, y_2, z_2 > 0$ since $a, b, m > 0$. We have $\gcd(x_2, y_2) = 1$ since $\gcd(a, b) = 1$.

Finally, $z_2^2 = m = a^2 + b^2 = x_2^4 + y_2^4$. And $z_2 \leqslant z_2^2 = m \leqslant m^2 = m^2 + n^2 = z_1$, a contradiction. □

Exercise.

38.1. Show $x^n + 1 = y^{n+1}$ has no integer solutions in x, y, n with $\gcd(x, n+1) = 1$ and $n > 1$.

– End of this course.[5]

[3] Let $d = \gcd(x, y)$. Since $d \mid x$ and $d \mid y$, it implies $d^4 \mid x^4 + y^4 = z^2$. It further implies $d^2 \mid z$. Write $x = x'd$, $y = y'd$, and $z = z'd^2$, then $x^4 + y^4 = z^2$ becomes $x'^4 + y'^4 = z'^2$.

[4] $\gcd(a, b, c) = 1 \not\Longrightarrow \gcd(a, b) = 1$ necessarily but $\gcd(a, b) = 1 \implies \gcd(a, b, c) = 1$.

[5] Administrative announcement: Final exam covers material up to this point.

LECTURE 39

Day Thirty-Nine

— 28.04.2017

Non-elementary number theory

For the ambitious, where does elementary number theory go beyond this point?

Analytic theory (Math 531) We have seen the prime number theorem in Lecture 4, which states for $\pi(x) = |\{p : p \leqslant x, p \text{ primes}\}|$, we have

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

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

Question: How is this proved?

We can rephrase the prime number theorem as $\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$, where $o\left(\frac{x}{\log x}\right)$ is the error term.[1]

Then another question is could we get a better error term?

The classic proof is an application of results from complex analysis, though an elementary proof does exist. (See [**AS49**] for the elementary proof.)

In calculus, we studied convergence of infinite series, e.g., $\sum_{n=1}^{\infty} a_n$.

Example 39.1. $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

Sketch of Proof. Consider integral $\int_1^\infty \frac{1}{x}\,dx = \ln x \,|_1^\infty$ and use comparison test. ■

For $s \in \mathbb{R}$, if $s > 1$, the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ however, converges. We define a function $\zeta(s)$, called **Riemann ζ-function** on $\{s \in \mathbb{R} : s > 1\}$ by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Example 39.2. $\zeta(2) = \frac{\pi^2}{6}$.

Sketch of Proof. This is called **Basel problem**. See its wikipedia entry and stack exchange discussion.[2] ■

A fact is that the infinite series defined in Riemann ζ-function also makes sense and converges as a complex number for any $s = x + iy \in \mathbb{C}$ with $x > 1$, $x, y \in \mathbb{R}$. As illustrated in the Figure 39.2, $\zeta(s)$ is defined on the shaded region. This function is very nice—it is continuous and holomorphic on the defined domain. (Holomorphic means complex differentiable, cf. Math 448.)

A less easy fact: There is a unique way to extend $\zeta(s)$ to a holomorphic function on $\{s \in \mathbb{C} : s \neq 1\}$.

[1] The little-o notation $f(x) = o(g(x))$ involving functions $f(x), g(x)$ means $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

[2] https://math.stackexchange.com/questions/8337/different-methods-to-compute-sum-limits-k-1-infty-frac1k2

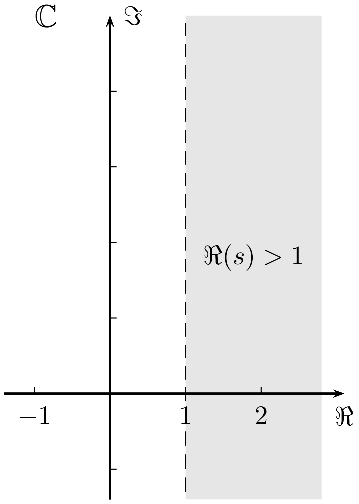

FIGURE 39.1. Region of convergence of $\zeta(s)$ on the complex plane.

THEOREM 39.3. *The prime number theorem is equivalent to the statement*

$$\zeta(1+iy) \neq 0 \text{ for any } y \neq 0.$$

This is how prime number theorem is usually proved.

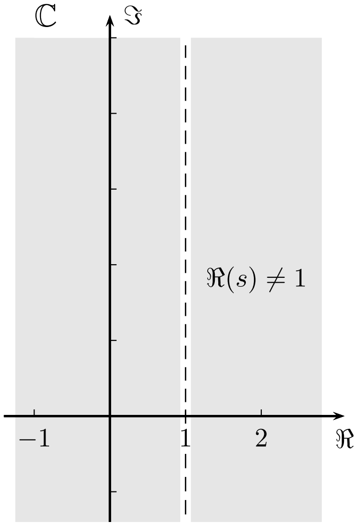

FIGURE 39.2. Extending $\zeta(s)$ on the entire complex plane except $s = 1$.

Question: How is $\zeta(s)$ connected to primes?

THEOREM 39.4 (Euler). *For $s = x + iy$, $x > 1$, we have*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

CONJECTURE 39.5 (Riemann hypothesis). *If $s = x + iy$ with $x \geqslant \frac{1}{2}$ satisfies $\zeta(s) = 0$, then $x = \frac{1}{2}$.*

The Riemann hypothesis is equivalent to a best possible error term for the prime number theorem. It says nontrivial zeros of Riemann ζ-function are concentrated on $x = \frac{1}{2}$ as seen in Figure 39.3.

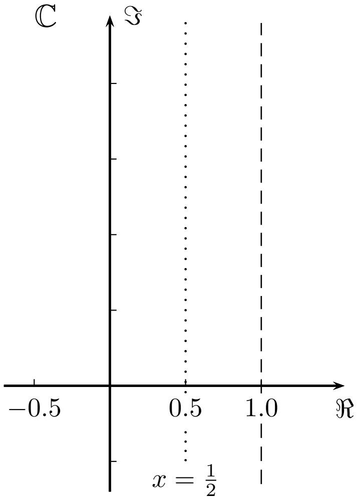

FIGURE 39.3. Nontrivial zeros of Riemann ζ-function are concentrated on $x = \frac{1}{2}$.

Let

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt,$$

we can show $\mathrm{Li}(x) \sim \frac{x}{\log x}$.

THEOREM 39.6 (Koch, 1901). *The Riemann hypothesis is equivalent to*

$$\pi(x) = Li(x) + \mathcal{O}(\sqrt{x}\log x).$$

Algebraic theory (Math 530)

A number α is called **algebraic** if it is a root of polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{Q}$.

EXAMPLE 39.7. Quick examples.

- $\sqrt{2}$ is algebraic since it is a root of $x^2 - 2$.
- π is not algebraic. It is not[3] obvious why it is not.

A number α is an **algebraic integer** if it is a root of a polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in \mathbb{Z}$.

EXAMPLE 39.8. Quick examples.

- $\sqrt{2}$ is an algebraic integer.
- $e^{\frac{2\pi i}{n}}$ with $n \geqslant 1$ is an algebraic integer since it is a n-th root of polynomial $x^n - 1$.

For α an algebraic integer, we study the number ring

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n : n \geqslant 1, a_i \in \mathbb{Z}\}.$$

We can add and multiply elements of $\mathbb{Z}[\alpha]$.

[3] Lindemann in 1882 gave the first proof. He first argued e^a is transcendental if a is algebraic, nonzero. By Euler's identity $e^{i\pi} = -1$ is algebraic. Therefore $i\pi$ must be transcendental. See [**Lin82**] for details.

Example 39.9. Primality tests in polynomial time use arithmetic in $\mathbb{Z}\left[e^{\frac{2\pi i}{n}}\right]$. We can define a prime element in $\mathbb{Z}[\alpha]$ by saying $x \in \mathbb{Z}[\alpha]$ is prime whenever $x \mid yz \implies x \mid y$ or $x \mid z$.

Question: With the notion of prime in Example 39.9, when does fundamental theorem of arithmetic hold in $\mathbb{Z}[\alpha]$? When is a prime p still prime in $\mathbb{Z}[\alpha]$?

Theorem 39.10. *A prime p is prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \bmod 4$.*

Remark 39.11. This result is very closely related to the first supplement to quadratic reciprocity, i.e., -1 is a square modulo an odd prime p if and only if $p \not\equiv 3 \bmod 4$. Generalizations of quadratic reciprocity go via this topic, i.e., asking how primes decompose or factor in rings like $\mathbb{Z}[\alpha]$.

Theorem 39.12 (Heegner–Stark). *There are only finitely many square free integers $d < 0$ such that fundamental theorem of arithmetic holds in $\mathbb{Z}[\sqrt{d}]$.*

Conjecture 39.13. *There are infinitely many square free integers $d > 0$ such that fundamental theorem of arithmetic holds in $\mathbb{Z}[\sqrt{d}]$.*

Day Forty

— 01.05.2017

Exercise session

EXERCISE 1. Let $a_1, a_2, \ldots, a_n, b \in \mathbb{Z}$. Consider the linear Diophantine equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b. \tag{40.1}$$

Show that

(1) if Equation (40.1) has a solution $x_i \in \mathbb{Z}$, then $\gcd(a_1, a_2, \ldots, a_n) \mid b$;
(2) if $\gcd(a_1, a_2, \ldots, a_n) \mid b$, then Equation (40.1) has infinitely many solutions.

(*Hint*: For Part (2), we can induct on n.)

EXERCISE 2. Let p be a prime and $d \mid p-1$. Let

$$f(d) = |\{1 \leqslant a \leqslant p-1 : \mathrm{ord}_p(a) = d\}|.$$

To prove primitive roots modulo p exist, we showed $f(d) = \varphi(d)$. This exercise gives another proof using Möbius inversion.

(1) Show $\sum_{\substack{c \mid d \\ c>0}} f(c) = d$.
(2) Show $f(d) = \sum_{\substack{c \mid d \\ c>0}} \mu(c)\frac{d}{c}$.
(3) Show $f(d) = \varphi(d)$.

(*Hint*: This problem is the same as [**Str01**, §5.2, Problem 20].)

EXERCISE 3. Let n, d be positive integers with $d \mid n$. Show that

(1) for any $a \in \mathbb{Z}$ with $\gcd(a, d) = 1$, there is a $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$ such that $b \equiv a \bmod d$;
(2) if r is a primitive root modulo n, then r is also a primitive root modulo d.

(*Hint*: Part (2) showed up before as Corollary 30.3. See also a stack exchange discussion.[1])

[1] https://math.stackexchange.com/questions/2307411/if-g-is-a-primitive-root-modulo-n-then-g-is-a-primitive-root-modulo-d-wher

Bibliography

[MAaNKaNS04] Manindra Agrawal and Neeraj Kayal and Nitin Saxena, *PRIMES Is in P*, Annals of Mathematics **160** (2004), no. 2, 781-793, DOI 10.4007/annals.2004.160.781.

[GT08] Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), no. 2, 481-547.

[TKCDaAKLaCPaCS17] Thorsten Kleinjung and Claus Diem and Arjen K. Lenstra and Christine Priplata and Colin Stahlke, *Computation of a 768-bit prime field discrete logarithm*, 2017. http://eprint.iacr.org/2017/067.

[Knu97] Donald E. Knuth, *The Art of Computer Programming, Volume 1 (3rd Ed.): Fundamental Algorithms*, Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1997.

[Ko80] Chao Ko, *100 Problems in Elementary Number Theory*, Education Press of Shanghai, 1980.

[Ko01] ———, *Lectures on Elementary Number Theory*, Vol. 1, Higher Education Press, 2001.

[Lin82] Ferdinand von Lindemann, *Ueber die Zahl π*, Mathematische Annalen **20** (1882), no. 2, 213–225, DOI 10.1007/BF01446522.

[MvdD04] Yiannis N. Moschovakis and Lou van den Dries, *Is the Euclidean algorithm optimal among its peers?*, Bull. Symbolic Logic **10** (2004), no. 3, 390–418, DOI 10.2178/bsl/1102022663.

[Rou91] G. Rousseau, *On the quadratic reciprocity law*, Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics **51** (1991), no. 3, 423425, DOI 10.1017/S1446788700034583.

[AS49] Atle Selberg, *An Elementary Proof of the Prime-Number Theorem*, Annals of Mathematics **50** (1949), no. 2, 305-313.

[Str01] James K. Strayer, *Elementary Number Theory*, Waveland Press, 2001.

[Web95] Kenneth Weber, *The Accelerated Integer GCD Algorithm*, ACM Trans. Math. Softw. **21** (1995), no. 1, 111–122, DOI 10.1145/200979.201042.