

Number Theory: Lecture Notes

Anthony Dunford Chris Nash

November 16, 2017

1 Divisibility and Primes

1.1 Introduction

Well ordering Principle:

Let $S \neq \emptyset$ be a set of positive integers.

Then there exists $s \in S$ such that for all $a \in S, s \leq a$

Induction:

If a set S of positive integers contains the integer 1

And contains $n + 1$ whenever it contains n

Then S consists of all the positive integers

1.2 Divisibility

Definition 1.1: Divisibility

An integer b is divisible by integer $a \neq 0$ if there is an integer x such that $b = ax$.

s We write $a|b$ (a divides b)

Theorem 1.1: Properties of divisibility

1. $a|b \rightarrow a|bc \quad c \in \mathbb{Z}$
2. $a|b \ \& \ b|c \rightarrow a|c$
3. $a|b \ \& \ a|c \rightarrow a|(bx + cy) \quad x, y \in \mathbb{Z}$
4. $a|b \ \& \ b|a \rightarrow a = \pm b$
5. $a|b, \ a > 0, \ b > 0 \rightarrow a \leq b$
6. $m \neq 0, \ a|b \leftrightarrow ma|mb$

Proof: Theorem 1.1 (3)

$a|b \rightarrow b = ar$ for some $r \in \mathbb{Z}$ and $a|c \rightarrow c = as$ for some $s \in \mathbb{Z}$ Hence $bx + cy = a(rx + sy)$ and this proves that $a|(bx + cy)$

Theorem 1.2: The Division Algorithm

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

Then there exists unique $q, r \in \mathbb{Z}$ such that $b = qa + r$, $0 \leq r < a$.

If $a \nmid b$ then $0 < r < a$

Proof: Theorem 1.2

Consider the arithmetic progression:

$$\dots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \dots$$

In the sequence select the smallest non-negative member and denote it by r . Thus by definition r satisfies the inequalities of the theorem. But also r , being in the sequence, is of the form $b - qa$, and thus q is defined in terms of r .

To prove uniqueness we suppose there is another pair q_1 and r_1 satisfying the same conditions. First we prove that $r = r_1$. If not, we may presume that $r < r_1$ so that $0 < r_1 - r < a$ and then we see that $r_1 - r = a(q - q_1)$ and so $a|(r_1 - r)$, a contradiction to Theorem 1.1 (5). Hence $r = r_1$ and also $q = q_1$.

Note: We stated the theorem with $a > 0$. However this is not necessary and we may formulate as:

Given $a, b \in \mathbb{Z}$, $a \neq 0$, there exists $q, r \in \mathbb{Z}$ such that $b = qa + r$, $0 \leq r < |a|$.

Definition 1.2:

The integer a is a common divisor of b and c if $a|b$, $a|c$ and at least $b \neq 0$ or $c \neq 0$, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by $\gcd(b, c)$ or (b, c) .

Let $b_1, \dots, b_n \in \mathbb{Z}$, not all zero. We denote $g = (b_1, \dots, b_n)$ to be the greatest common divisor.

Theorem 1.3:

If $g = (b, c)$, then there exist $x_0, y_0 \in \mathbb{Z}$ such that $g = (b, c) = bx_0 + cy_0$

Proof: Theorem 1.3

Consider the linear combination $bx + cy$, where x, y range over all the integers. This set of integers $\{bx + cy\}$ includes positive and negative values and also 0. ($x = y = 0$). Choose x_0 and y_0 so that $bx_0 + cy_0$ is the least positive integer l in the set. Thus $l = bx_0 + cy_0$.

Next we prove that $l|b$ and $l|c$. Assume that $l \nmid b$, then it follows that there exists integers q and r , by Theorem 1.2, such that $b = lq + r$ with $0 < r < l$. Hence we have $r = b - lq = b - q(bx_0 + cy_0) = b(l - qx_0) + c(-qy_0)$, and thus r is in the set $\{bx + cy\}$. This contradicts the fact that l is the least positive integer

in $\{bx + cy\}$. Similar proof for $l|c$. Now since $g = (b, c)$ we may write $b = gB$, $c = gC$ and $l = bx_0 + cy_0 = g(Bx_0 + Cy_0)$. Thus $g|l$ and so by Theorem 1.1 (5) we conclude that $g \leq l$. We know $g < l$ is impossible since g is the greatest common divisor, so $g = l = bx_0 + cy_0$.

Theorem 1.4:

The greatest common denominator of b and c can be characterised in the following two ways:

1. It is the least positive value of $bx + cy$ where $x, y \in \mathbb{Z}$
2. If d is any common divisor of b and c then $d|g$ by Theorem 1.1 (3).

Proof: Theorem 1.4

1. Follows from Theorem 1.3
2. If d is any common divisor of b and c , then $d|g$ by Theorem 1.1 (3). Moreover, there cannot be two distinct integers with property (2), because of Theorem 1.1 (4).

Note: If $d = bx + cy$, then d is not necessary the $\gcd(b, c)$. However, it does follow from such align that (b, c) is a divisor of d . In particular, if $bx + cy = 1$ for some $x, y \in \mathbb{Z}$, then $(b, c) = 1$.

Theorem 1.5:

Given $b_1, \dots, b_n \in \mathbb{Z}$ not all zero with greatest common divisor g , there exists integers x_1, \dots, x_n , such that

$$g = (b_1, \dots, b_n) = \sum_{j=1}^n b_j x_j \quad (1)$$

Furthermore, g is the least positive value of the linear form $\sum_{j=1}^n b_j y_j$ where the y_j runs over all integers; also g is the positive common divisor of b_1, \dots, b_n that is divisible by every common divisor.

Proof: Theorem 1.5

Exercise for the reader.

Theorem 1.6:

For any $m \in \mathbb{Z}, m > 0$

$$(ma, mb) = m(a, b) \quad (2)$$

Proof: Theorem 1.6

By Theorem 1.4 we have:

$(ma, mb) = \text{least positive value of } max + mby = m \{ \text{least positive integer of } ax + by \} = m(a, b)$

Theorem 1.7:

If $d|a$, $d|b$ and $d > 0$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) \quad (3)$$

If $(a, b) = g$, then

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1 \quad (4)$$

Proof: Theorem 1.7

The second assertion is the special case of the first using $d = (a, b) = g$. The first assertion is a direct consequence of Theorem 1.6, obtained by replacing m, a, b in Theorem 1.6 by $d, \frac{a}{d}, \frac{b}{d}$ respectively.

Theorem 1.8:

If $(a, m) = (b, m) = 1$ then $(ab, m) = 1$

Proof: Theorem 1.8

Exercise for the reader.

Definition: 1.3

We say that a and b are relatively prime in case $(a, b) = 1$, and that a_1, a_2, \dots, a_n are relatively prime in the case $(a_1, a_2, \dots, a_n) = 1$. We say that a_1, a_2, \dots, a_n are relatively prime in pairs in case $(a_i, a_j) = 1$ for all $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, n$ with $i \neq j$.

Note: $(a, b) = 1$ we also say a and b are coprime.

Theorem 1.9:

For any $x \in \mathbb{Z}$ we have

$$(a, b) = (b, a) = (a, -b) = (a, b + ax) \quad (5)$$

Proof: Theorem 1.9

Exercise for the reader.

Theorem 1.10: Euclid's Lemma

If $c|ab$ and $(b, c) = 1$, then $c|a$.

Proof: Theorem 1.10

By Theorem 1.6, $(ab, ac) = a(b, c) = a$. By hypothesis $c|ab$ and clearly $c|ac$, so $c|a$ by Theorem 1.4 (2).

Now we observe for $c \neq 0$, we have $(b, c) = (b, -c)$ by Theorem 1.9 and hence we may presume $c > 0$.

Theorem 1.11: The Euclidean Algorithm

Given $b, c \in \mathbb{Z}, c > 0$, we can make a repeated application of the division algorithm, **Theorem 1.2**, to obtain a series of aligns

$$b = cq_1 + r_1 \quad 0 < r_1 < c \quad (6)$$

$$c = r_1q_2 + r_2 \quad 0 < r_2 < r_1 \quad (7)$$

$$r_1 = r_2q_3 + r_3 \quad 0 < r_3 < r_2 \quad (8)$$

$$\dots \quad (9)$$

$$r_j = r_{j+1}q_j + r_j \quad 0 < r_j < r_{j-1} \quad (10)$$

$$r_{j-1} = r_jq_{j+1}. \quad (11)$$

The greatest common divisor (b, c) of b and c is r_j , the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b, c) = bx_0 + cy_0$ can be obtained by writing each r_i as a linear combination of b and c .

Proof: Theorem 1.11

See Theorem 1.11 in the textbook or Theorem 1.13 in the Lecture Notes.

Example 1 $\gcd(841, 160)$

$$\begin{aligned} 841 &= 160 \times 5 + 41 \\ 160 &= 41 \times 3 + 37 \\ 41 &= 37 \times 1 + 4 \\ 37 &= 34 \times 9 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned} \quad (12)$$

Hence $(841, 160) = 1$ working backwards gives:

$$1 = 37 \times 1 - 4 \times 9 \quad (13)$$

$$1 = 37 \times 1 - (41 - 37) \times 9 \quad (14)$$

$$1 = 37 \times 10 - 41 \times 9 \quad (15)$$

$$1 = (160 - 3 \times 41) \times 10 - 41 \times 9 \quad (16)$$

$$1 = 160 \times 10 - 41 \times 39 \quad (17)$$

$$1 = 160 \times 10 - (841 - 160 \times 5) \times 39 \quad (18)$$

$$1 = (-39) \times 841 + 205 \times 160 \quad (19)$$

$$(20)$$

Note the solution is not unique:

$$1 = 121 \times 841 - 636 \times 160 \quad (21)$$

Example 2 Extended Algorithm

$$\begin{aligned}
r_i &= r_{i-2} - q_i r_{i-1} \\
x_i &= x_{i-2} - q_i x_{i-1} \\
y_i &= y_{i-2} - q_i y_{i-1} \\
r_1 &= b, r_0 = c \\
x_1 &= 1, x_0 = 0 \\
y_1 &= 0, y_0 = 1
\end{aligned} \tag{22}$$

We want to compute the $\gcd(841, 160)$ and express as a linear combination of 841 and 160.

Definition 1.4:

The integers a_1, \dots, a_n , all different from zero, have a **common multiple** b if $a_i | b$ for $i = 1, \dots, n$. The least of the positive common multiples is called the **least common multiple** and it is denoted by $[a_1, \dots, a_n]$ or $\text{lcm}(a_1, \dots, a_n)$

Theorem 1.12:

If b is any common multiple of a_1, \dots, a_n , then $[a_1, \dots, a_n] | b$. This is the same as saying that if $h = [a_1, \dots, a_n]$ then $0, \pm h, 2 \pm h, \dots$ comprise all the common multiples of a_1, \dots, a_n .

Proof: Theorem 1.12

Let m be any common multiple and divide m and h . By Theorem 1.2, $\exists q, r$ such that $m = qh + r$, $0 \leq r < h$. We must prove that $r = 0$. If $r \neq 0$ we argue as follows. For each $i = 1, 2, \dots, n$ we know that $a_i | h$ and $a - i | m$, so that $a_i | r$. Thus r is a positive common multiple of a_1, a_2, \dots, a_n contrary to the fact that h is the least of all positive common multiples.

Theorem 1.13:

If $m > 0$

1. $[ma, mb] = m[a, b]$
2. $a, b = |ab|$

Proof: Theorem 1.13

1. Let $H = [ma, mb]$ and $h = [a, b]$. Then mh is a multiple of ma and mb , so that $mh \geq H$. Also, H is a multiple of both ma and mb so H/m is a multiple of a and b . Thus, $H/m \geq h$ from which it follows that $mh = H$.
2. It will suffice to prove this for $a, b \in \mathbb{Z}$ with $a > 0, b > 0$, since $[a, -b] = [a, b]$. We begin with the special case where $(a, b) = 1$. Now $[a, b] = 1$, is a multiple of a , say ma . Then $b | ma$ and $(a, b) = 1$, so by Theorem 1.10 we conclude that $b | m$. Hence $b \leq m$, $ba \leq ma$. But ba , being a positive

common multiple of a and b , cannot be less than the least common multiple, so $ba = ma = [a, b]$.

Let $(a, b) = g > 1$. we have $(a/g, b/g) = 1$ by Theorem 1.7. Applying the result of the previous paragraph we have:

$$[a/g, b/g] \cdot (a/g, b/g) = ab/g \quad (23)$$

Multiplying by g^2 and using Theorem 1.6 as well as the first part (1.), we get $[a, b] \cdot (a, b) = ab$.

1.3 Primes

Definition 1.5:

An integer $p > 1$ is called a **prime number** if there is no divisor d of p satisfying $1 < d < p$. If an integer $a > 1$ is not a prime, it is called a **composite number**.

Theorem 1.14:

Every integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor).

Theorem 1.15:

If $p|ab$, p prime, then $p|a$ or $p|b$. More generally if $p|a_1 \dots a_n$, then p divides at least one of the factors a_i . If $p \nmid a$, then $(a, p) = 1$ and so by **Thm 1.10**, $p|b$. For the general case, we use induction.

Theorem 1.16: Fundamental Theorem of Arithmetic

The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.

Definition 1.6:

We call a a square (or **perfect square**) if it can be written as $a = n^2$. By the **F.T.A.** a is a square if all the exponents $\alpha(p)$ in (1.6) are even. We say that a is **square free** if 1 is the largest square dividing a . Thus a is square free iff the exponents $\alpha(p) = 0$ or 1. If p is prime, then the assertion $p^k || a$ is equivalent to $k = \alpha(p)$.

Theorem 1.17: (Euclid)

The number of primes is infinite.

Definition 1.7:

Let $n \in \mathbb{N}$ and p a prime. Then

$$v_p(n) = \max(k \in \mathbb{N}_{\geq 0} : p^k | n) \quad (24)$$

where k is the unique non-negative integer such that $p^k | n$ but $p^{k+1} \nmid n$. Equivalently $V_p(n) = k$ iff $n = p^k n'$ where $n' \in \mathbb{N}$ and $p \nmid n'$.

Lemma: Let $n, m \in \mathbb{N}$ and p be a prime. then

$$v_p(mn) = v_p(m) + v_p(n) \quad (25)$$

2 Congruences

2.1 Congruences

Definition 2.1:

If $m \in \mathbb{Z}$, $m \neq 0$ is such that $m|a - b$, we say that a is congruent to b modulo m and we write $a \equiv b \pmod{m}$

Since $a - b$ is divisible by $-m$, we can focus our attention to a positive modulus. We will assume in this chapter that $m > 0$.

Theorem 2.1: Properties of Congruences

1. $a \equiv b \pmod{m}$ $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$
5. If $a \equiv b \pmod{m}$ and $d|m$, $d > 0$, then $a \equiv b \pmod{d}$
6. If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c > 0$

Theorem 2.2:

Let f denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$ then $f(a) \equiv f(b) \pmod{m}$

Theorem 2.3:

1. If $ax \equiv by \pmod{m}$ and $x \equiv y \pmod{\text{fracm}(a, m)}$
2. $ax \equiv by \pmod{m}$ and $(a, m) = 1$, then $x \equiv y \pmod{m}$
3. $x \equiv y \pmod{m_i}$ for $i = 1, \dots, r$ iff $x \equiv y \pmod{[m_1, \dots, m_r]}$

Definition 2.2:

If $x \equiv y \pmod{m}$ then y is called a residue of $x \pmod{m}$. A set x_1, \dots, x_m is called a complete residue system modulo m if for every integer y , there is one and only one x_j such that $y \equiv x_j \pmod{m}$

Theorem 2.4:

If $b \equiv c \pmod{m}$, then $(b, m) = (c, m)$.

Definition 2.3:

A reduced residue system modulo m is a set of integers r_i such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m (coprime) is congruent modulo m to some member r_i of the set.

- You can obtain a reduced residue system by deleting from a complete residue system modulo m those members that are not relatively prime to m .
- We will denote by $\Phi(m)$ to be the number of elements of a reduced residue system modulo m .
- All reduced residue systems modulo m have the same number of elements.
- $\Phi(m)$ is called the Euler's Φ -function or Euler's totient-function

Theorem 2.5:

The number $\Phi(m)$ is the number of positive integers less than or equal to m are relatively prime to m .

Theorem 2.6:

Let $(a, m) = 1$. Let r_1, \dots, r_n be a complete, or a reduced, residue system modulo m . Then ar_1, \dots, ar_n is a complete, or a reduced, residue system, respectively, modulo m .

Theorem 2.7: Fermat's Theorem

Let p denote a prime. If $p \nmid a$ then
 $a^{p-1} \equiv 1 \pmod{p}$. For every integer a ,
 $a^p \equiv a \pmod{p}$.

Theorem 2.8: Euler's Generalization of Fermat's Theorem

If $(a, m) = 1$, then

$$a^{\Phi(m)} \equiv 1 \pmod{m} \quad (26)$$

Theorem 2.9:

If $(a, m) = 1$ then there is an x such that $ax \equiv 1 \pmod{m}$. Any two such x are congruent \pmod{m} . If $(a, m) > 1$ then there is no such x .

Lemma 2.10:

Let p be a prime number. Then $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$.

Theorem 2.11: Wilson's Theorem

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$

Theorem 2.12:

Let p denote a prime. Then $x^2 \equiv -1 \pmod{p}$ has solutions iff $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof: Theorem

Theorem 2.13:

If p is prime and $p \equiv 1 \pmod{4}$, then there exists positive integers a and b such that $a^2 + b^2 = p$.

Lemma 2.14:

Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \pmod{4}$ then $q|a$ and $q|b$.

Theorem 2.15: (Fermat)

Let

$$n = 2^\alpha \prod_{p \equiv 1(4)} p^\beta \prod_{q \equiv 3(4)} q^\gamma \quad (27)$$

Then n can be expressed as a sum of two squares iff all the exponents of γ are even.

2.2 Solutions of Congruences

- Let $f(x)$ denote a polynomial, e.g.

$$f(x) = a_n x^n + \dots + a_0 \quad (28)$$

- if $u \in \mathbb{Z}$ such that $f(u) \equiv 0 \pmod{m}$ then we say that u is a solution of the congruence $f(x) \equiv 0 \pmod{m}$
- If u is a solution of $f(x) \equiv 0 \pmod{m}$ and if $v \equiv u \pmod{m}$, then theorem 2.2 shows that v is also a solution.
 - $x \equiv u \pmod{m}$ is a solution of $f(x) \equiv 0 \pmod{m}$ meaning that every integer congruent to u modulo m satisfied $f(x) \equiv 0 \pmod{m}$.

Definition 2.4:

Let r_1, \dots, r_m denote a complete residue system modulo m .

The number of solutions of $f(x) \equiv 0 \pmod{m}$ is the number of the r_i such that $f(r_i) \equiv 0 \pmod{m}$

Definition 2.5:

Let $f(x) = a_n x^n + \dots + a_0$. If $a_n \equiv 0 \pmod{m}$ the degree of the congruence $f(x) \equiv 0 \pmod{m}$ is n . If $a_n \not\equiv 0 \pmod{m}$, let j be the largest integer such that $a_j \not\equiv 0 \pmod{m}$; then the degree of the congruence is j . If there is no such integer j , then no degree is assigned to the congruence.

Theorem 2.16:

If $d|m$, $d > 0$, and if u is a solution of $f(x) \equiv 0 \pmod{m}$, then u is a solution of $f(x) \equiv 0 \pmod{d}$

- We say that $f(x) \equiv 0 \pmod{m}$ is an identical congruence if it holds for all integers x
 - If $f(x)$ is a polynomial whose coefficients are divisible by m , then $f(x) \equiv 0 \pmod{m}$ is an identical congruence
 - e.g. $x^p \equiv x \pmod{p}$ is true for all integers x by theorem 2.5

Theorem 2.17: Linear Congruences

Let a, b and $m > 0$ be given integers, and put $g = (a, m)$. The congruence $ax \equiv b \pmod{m}$ has a solution iff $g|b$. If this condition is met, then the solution forms an arithmetic progression with common difference $\frac{m}{g}$, giving g solutions \pmod{m} .

How to solve general linear congruences: Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose we wish to solve the linear congruence

$$ax \equiv b \pmod{n} \quad (29)$$

Firstly apply the Extended Euclidean Algorithm to compute $d = \gcd(a, n)$ and find $x', y' \in \mathbb{Z}$ such that

$$ax' + ny' = d \quad (30)$$

If $d \nmid b$ then there are no solutions by theorem 2.17. Otherwise, there are exactly d solutions modulo n by theorem 2.17, which we can find as follows.

Write

$$a = da', \quad b = db', \quad n = dn' \quad (31)$$

Dividing (18) by d gives

$$a'x' + n'y' = 1 \quad (32)$$

Thus reducing mod n' gives $a'x' \equiv 1 \pmod{n'}$ and multiplying by b' gives $a'(b'x') \equiv b' \pmod{n'}$. Therefore $t := b'x'$ is the unique solution to $a'x \equiv b' \pmod{n'}$. Now by theorem 2.17 the solutions to (17) are $t, t+n', \dots, t+(d-1)n'$

2.3 The Chinese Remainder Theorem

Solve Simultaneous Congruences

Find x (is there are any) that satisfies

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_r \pmod{m_r} \end{aligned} \quad (33)$$

Theorem 2.18: The Chinese Remainder Theorem

Let m_1, \dots, m_r denote r positive integers that are relatively prime in pairs, and let $a_1, \dots, a_r \in \mathbb{Z}$. Then the congruences (21) have have common solutions. If x_0 is one such solution, then an integer x satisfies the congruences (21) iff $x = x_0 + km$ for some integer k . Here $m = m_1 m_2 \dots m_r$.

- m_1, \dots, m_r positive integers relatively prime in pairs

- $m = m_1 m_2 \dots m_r$
- Instead of considering just one set of aligns (21), we will consider all possible systems of this type
- Let

$$\begin{aligned}
a_1 &\in \{1, \dots, m_1\} \\
a_2 &\in \{1, \dots, m_2\} \\
&\dots \\
a_r &\in \{1, \dots, m_r\}
\end{aligned} \tag{34}$$

- The number of such r -tuples (a_1, \dots, a_r) is $m = m_1 m_2 \dots m_r$.
- By the **C.R.T.** each r -tuple determines precisely one residue class x modulo m .
 - Moreover, distinct r -tuples determine different residue classes. To see this, suppose that $(a_1, \dots, a_r) \neq (a'_1, \dots, a'_r)$. then $a_i \neq a'_i$ for some i , and we see that no integer x satisfies both the congruences $x \equiv a_i \pmod{m_i}$ and $x \equiv a'_i \pmod{m_i}$
- This we have a one-to-one correspondence between the r -tuples (a_1, \dots, a_r) and a complete residue system modulo m , such as the integers $1, \dots, m$

Theorem 2.19:

If $m_1, m_2 > 0$, $(m_1, m_2) = 1$, then $\phi(m_1 m_2) = \phi(m_1) \phi(m_2)$ moreover, if $m = \prod p^\alpha$ then

$$\phi(m) = \prod_{p|m} (p^\alpha - p^{\alpha-1}) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) \tag{35}$$

Theorem 2.20:

Let $f(x)$ be a fixed polynomial with integral coefficients, and for any positive integer m let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1) N(m_2)$. If $m = \prod p^\alpha$, then $N(m) = \prod N(p^\alpha)$

2.4 Public-key Cryptography

Lemma 2.22:

Suppose $m \in \mathbb{Z}$, $m > 0$, $(a, m) = 1$. If $k, \bar{k} \in \mathbb{Z}$ and $k, \bar{k} > 0$ such that $k, \bar{k} \equiv 1 \pmod{\phi(m)}$, then $a^{k\bar{k}} \equiv a \pmod{m}$.

Proof: Theorem 2.22

Write $k\bar{k} = 1 + r\phi(m)$ for some $r \in \mathbb{Z}$. Then by Euler's congruence

$$a^{k\bar{k}} = a a^{r\phi(m)} = a(a^{\phi(m)})^r \equiv a \cdot 1^r = a \pmod{m}$$

- If $(a, m) = 1$, $k > 0$, then $(a^k, m) = 1$. Thus if $n = \phi(m)$ and r_1, \dots, r_n is a system of reduced residues $(\text{mod } m)$, then the numbers r_1^k, \dots, r_n^k are also relatively prime to m . These k^{th} powers may not all be distinct $(\text{mod } m)$, as we see by considering the case $k = \phi(m)$. On the other hand, from lemma 2.22, we can deduce that these k^{th} powers are distinct $(\text{mod } m)$ provided that $(k, \phi(m)) = 1$.
- Suppose that $r_i^k \equiv r_j^k \pmod{m}$ and $(k, \phi(m)) = 1$. By theorem 2.9 we may find $\bar{k} > 0$ such that $k\bar{k} \equiv 1 \pmod{\phi(m)}$ and then it follows from the lemma that

$$r_i \equiv r_i^{k\bar{k}} = (r_i^k)^{\bar{k}} \equiv (r_j^k)^{\bar{k}} = r_j^{k\bar{k}} \equiv r_j \pmod{m} \quad (36)$$

This implies that $i = j$. We will show later that the converse also holds: the numbers r_1^k, \dots, r_n^k are distinct $(\text{mod } m)$ only if $(k, \phi(m)) = 1$. Suppose that $(k, \phi(m)) = 1$. Since the numbers r_1, \dots, r_n are distinct $(\text{mod } m)$, they form a system of reduced residues $(\text{mod } m)$. That is the map $a \mapsto a^k$ permutes the reduced residues $(\text{mod } m)$ if $(k, \phi(m)) = 1$. The significance of the lemma is that the further map $b \mapsto b^{\bar{k}}$ is the inverse permutation.

- To apply these observations to cryptography, we take two distinct large primes, p_1, p_2 , say each one with about 100 digits.
 - So $m = p_1 p_2$ has about 200 digits.
 - Since we know the prime factorisation of m , from theorem 2.19 we have that $\phi(m) = (p_1 - 1)(p_2 - 1)$
 - So $\phi(m) < m$
 - we choose now a big number k , $0 < k, \phi(m)$ and check by the Euclidean algorithm that $(k, \phi(m)) = 1$. We try until we get such a k .
 - We make the numbers m and k publicly available, by keep p_1, p_2 and $\phi(m)$ secret.
 - suppose now thatt some associate of ours wants to send us a message, say '*Gauss was a genius!*'. The associate first converts the characters to number in some standard way, say by emplying (ASCII). Then $G = 071$, $a = 097, \dots$, $! = 033$. Then concatenate these codes to form a number

$$a = 071097117115115126119097115126097126103101110105117115033$$

- if the message were longer, it could be ficed into a number of blocks.
- the associate could send the number a and we could reconstruct the message. But suppose that message has some sensitive information. In that case the associate would use the number k and m that we have provided.
- Our associate quickly finds the unique number b , $0 \leq b < m$ such that $b \equiv a^k \pmod{m}$ and sends this b to us.
- We use Euclidean Algorithm to find $\bar{k} > 0$ such that $k\bar{k} \equiv 1 \pmod{\phi(m)}$ and then we find the unique c such that $0 \leq c < m$, $c \equiv b^{\bar{k}} \pmod{m}$. From lemma 2.22 we deduce that $a = c$.

- In theory it might happen that $(a, m) > 1$ in which case the lemma does not apply, but the chances of this is $\approx \frac{1}{p_i} \approx 10^{-100}$. Suppose that some third party gain access to the numbers m , k and b , and seeks to recover the number a . In principle, all that needs to be done is to factor m , which yields $\phi(m)$, and hence \bar{k} . The problem of locating the factors of m for a big number is not easy.

2.5 Prime Power Moduli

Let $f(x)$ be a polynomial with integer coefficients. Let $N(m)$ denote the number of solutions of $f(x) \equiv 0 \pmod{m}$. Suppose that $m = m_1 m_2$, where $(m_1, m_2) = 1$. With a "little work", theorem 2.19 shows that the roots of the congruence $f(x) \equiv 0 \pmod{m}$ are in one-to-one correspondence with pairs (a_1, a_2) in which a_1 runs over all roots of the congruences $f(x) \equiv 0 \pmod{m_1}$ and a_2 runs over all roots of the congruence $f(x) \equiv 0 \pmod{m_2}$.

- From theorem 2.16 and theorem 2.20 we have that the congruence $f(x) \equiv 0 \pmod{m}$ has solutions iff it has solutions $\pmod{p^\alpha}$ for each prime power p^α exactly dividing m .

Example: Let $f(x) = x^2 + x + 7$. Find all roots of $f(x) \equiv 0 \pmod{189}$, given that $189 = 3^3 \cdot 7$, that all roots $\pmod{27}$ are 4, 13, and 22, and that the roots $\pmod{7}$ are 0 and 6.

Solution: By the Euclidean algorithm and (2.2), we find that $x \equiv a_1 \pmod{27}$ and that $x \equiv a_2 \pmod{7}$ iff $x \equiv 28a_1 - 27a_2 \pmod{189}$. We let $a_1 = 4, 13, 22$ and $a_2 = 0, 6$. Thus we obtain the six solutions 13, 49, 76, 112, 139, 175 $\pmod{189}$.

- The problem of solving a congruence is now reduced to the case of a prime-power modulus.
 - To solve $f(x) \equiv 0 \pmod{p^k}$ we start with a solutions modulo p and then move to p^2, p^3, \dots, p^k .

Suppose that $x = a$ is a solution of $f(x) \equiv 0 \pmod{p^j}$ and we want to use it to get a solution modulo p^{j+1} . The idea is to try to get a solution $x = a + tp^j$, where t is to be determined, by use of Taylor's expansion

$$f(a + tp^j) = f(a) + tp^j f'(a) + \frac{t^2 p^{2j}}{2!} f''(a) + \dots + \frac{t^n p^{nj}}{n!} f^{(n)}(a) \quad (37)$$

where $n = \text{degree of } f(x)$. All derivatives beyond the n^{th} are identically zero. Now with respect to the modulus p^{j+1} , equation (37) gives

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

as the following argument shows. What we want to establish is that the coefficients of t^1, t^3, \dots, t^n in (37) are divisible by p^{j+1} and so can be omitted in (38). This is almost obvious because the powers of p in those

terms. The explanation is that $\frac{f^{(k)}(a)}{k!}$ is an integer for each value of k , $2 \leq k \leq n$. To see this, let cx^r be a representative term from $f(x)$. The corresponding term in $f^{(k)}(a)$ is $cr(r-1)(r-2)\dots(r-k+1)a^{r-k}$.

We now use the fact (without proof), that the product of k consecutive integers is divisible by $k!$, and the argument is complete. Thus, we have proved that the coefficients of t^2, t^3, \dots, t^n in (37) are divisible by p^{j+1} . The congruence (38) reveals how t should be chosen if $x = a + tp^j$ is to be a solution of $f(x) \equiv 0 \pmod{p^{j+1}}$. We want t to be a solution of

$$f(a) + tp^j f'(a) \equiv 0 \pmod{p^{j+1}} \quad (38)$$

Since $f(x) \equiv 0 \pmod{p^j}$ have the solutions $x = a$, we see that p^j can be removed as a factor to given

$$tf'(a) \equiv -\frac{f(a)}{p^j} \pmod{p} \quad (39)$$

Which is a linear congruence in t . This congruence may have no solution, one solutions, or p solutions. If $f'(a) \equiv 0 \pmod{p}$, then this congruence has exactly one solution, and we obtain

Theorem 2.3: Hensel's Lemma:

Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$ then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$

- If $f(a) \equiv 0 \pmod{p^j}$, $f(b) \equiv 0 \pmod{p^k}$, $j < k$ and $a \equiv b \pmod{p^j}$, then we say that b lies above a , or a lifts to b .
- If $a \equiv b \pmod{p^j}$, then a is called a nonsingular root if $f'(a) \not\equiv 0 \pmod{p}$; otherwise it is singular.
- By Hensel's lemma we see that a nonsingular root $a \pmod{p}$ lifts to a unique root $a_2 \pmod{p^2}$. Since $a_2 \equiv a \pmod{p}$ it follows by theorem 2.2 that $f'(a_2) \equiv f'(a) \not\equiv 0 \pmod{p}$. By a second application of Hensel's lemma we may lift a_2 to form a root a_3 of $f(x)$ modulo p^3 , and so on.
- In general we find that a nonsingular root a modulo p lifts to a unique root a_j modulo p^j for $j = 2, 3, \dots$ by (2.5) we see that this sequence is generated by means of the recursion

$$a_{j+1} = a_j - \frac{f(a_j)}{f'(a)} \pmod{p^{j+1}} \quad (40)$$

where $f'(a)$ is an integer chosen so that $f'(a) \overline{f'(a)} \equiv 1 \pmod{p}$.

Example: Solve $x^2 + x + 47 \equiv 0 \pmod{7^3}$

Solution: First we note that $x \equiv 1 \pmod{7}$ and $x \equiv 5 \pmod{7}$ are the only solutions of $x^2 + x + 47 \equiv 0 \pmod{7}$. Since $f'(x) = 2x + 1$, we see that

- $f'(1) = 3 \equiv 0 \pmod{7}$
- $f'(5) = 11 \equiv 0 \pmod{7}$

(So these roots are non singular)

Taking $f'(1) = 5$, we see by (40) that the root $a \equiv 1 \pmod{7}$ lifts to $a_2 = 1$. Since a_2 is considered $\pmod{7^2}$, we may take instead $a_2 = 1$. Then $a_3 = 1 - 49 \cdot 5 \equiv 99 \pmod{7^3}$. Similarly, we take $\overline{f'(5)} = 2$ and see by (40) that the root $5 \pmod{7}$ lifts to $5 - 77 \cdot 2 = -149 \equiv 47 \pmod{7^2}$ and that $47 \pmod{7^2}$ lifts to $47 - f(47) \cdot 2 = 47 - 2303 \cdot 2 = -4599 \equiv 243 \pmod{7^3}$. Thus we conclude that 99 and 243 are the desired roots and that there are no others.

2.6 Prime Modulus

$f(x) \equiv 0 \pmod{m} \rightarrow f(x) \equiv 0 \pmod{p}$ (reduced)
(No general method exists to solve such congruences)

Question:

Given a polynomial congruence $f(x) \equiv 0 \pmod{m}$ is there an analogue to the result in algebra which says that a polynomial equation of degree n with complex coefficients has exactly n roots?

→ for congruences the solution is more complicated.

e.g. For any $m > 1$, there are $f(x)$ such that $f(x) \equiv 0 \pmod{m}$ has no solutions.

e.g. $x^p - x + 1 \equiv 0 \pmod{m}$, where p is a prime factor of m has no solutions because $x^p - x + 1 \equiv 0 \pmod{p}$ has none, by Fermat's Theorem.

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ and we assume $p \nmid a_n$ so that the congruence $f(x) \equiv 0 \pmod{p}$ has degree n .

Theorem 2.25:

If the degree n of $f(x) \equiv 0 \pmod{p}$ is greater than or equal to p , then either every integer is a solution of $f(x) \equiv 0 \pmod{p}$ or there is a polynomial $g(x)$ having integral coefficients, with leading coefficient 1, such that $g(x) \equiv 0 \pmod{p}$ is of degree less than p and the solutions of $g(x) \equiv 0 \pmod{p}$ are precisely those of $f(x) \equiv 0 \pmod{p}$.

Proof: Theorem 2.25

Dividing $f(x)$ by $x^p - x$ we get a quotient $q(x)$ and a remainder $r(x)$ such that $f(x) = (x^p - x)q(x) + r(x)$. here $q(x)$ and $r(x)$ are polynomials with integral coefficients, and $r(x) = 0$ or degree $r(x) < p$. Since every integer is a solutions of $x^p \equiv x \pmod{p}$ are the same as those of $r(x) \equiv 0 \pmod{p}$ by Fermat's theorem, we see that the solutions of $f(x) \equiv 0 \pmod{p}$ are the same as those of $r(x) \equiv 0 \pmod{p}$. If $r(x) = 0$ or if every coefficient of $r(x)$ is divisible by p , then every integer is a solution of $f(x) \equiv 0 \pmod{p}$.

On the other hand, if at least one coefficient of $r(x)$ is not divisible by p , then the congruence $r(x) \equiv 0 \pmod{p}$ has a degree, and that degree is less than p . The

polynomial $g(x)$ in the theorem can be obtained from $r(x)$ by getting leading coefficient 1, as follows. We may discard all terms in $r(x)$ whose coefficients are divisible by p , since the congruence properties modulo p are unaltered. Then let bx^m be the term of the highest degree in $r(x)$, with $(b, p) = 1$. Choose \bar{b} so that $b\bar{b} \equiv 1 \pmod{p}$, and note that $(\bar{b}, b) = 1$ also. Then the congruence $\bar{b}r(x) \equiv 0 \pmod{p}$ has the same solutions as $r(x) \equiv 0 \pmod{p}$, and so has the same solutions as $f(x) \equiv 0 \pmod{p}$. Define $g(x) = \bar{b}r(x)$ with its leading coefficient $b\bar{b}$ replaced by 1, that is,

$$g(x) = \bar{b}r(x) - (b\bar{b} - 1)x^m \quad (41)$$

Theorem 2.26:

The congruence $f(x) \equiv 0 \pmod{p}$ of degree n has at most n solutions.

Proof: Theorem 2.26

The proof is by induction on the degree of $f(x) \equiv 0 \pmod{p}$. If $n = 0$, the polynomial $f(x) = a_0$ with $a_0 \not\equiv 0 \pmod{p}$ and hence the congruence has no solutions. If $n = 1$, the congruence has exactly one solutions by theorem 2.17. Assume the truth of the theorem for all congruences of degree $< n$, suppose that there were more than n solutions of the congruence $f(x) \equiv 0 \pmod{p}$ of degree n . Let the leading term of $f(x)$ be $a_n x^n$ and let u_1, \dots, u_{n+1} be solutions of the congruence with $u_i \not\equiv u_j \pmod{p}$ for $i \neq j$. We define $g(x)$ by

$$g(x) = f(x) - a_n(x - u_1)\dots(x - u_n) \quad (42)$$

noting the cancellation of $a_n x^n$ on the right.

Note that $g(x) \equiv 0 \pmod{p}$ has at least n solutions, namely u_1, \dots, u_n . We consider two cases:

- i. every coefficient. of $g(x)$ is divisible by p
- ii. at least one coefficient is not divisible by p

For (i), every integer is a solution of $g(x) \equiv 0 \pmod{p}$, and since $f(u_{n+1}) \equiv 0 \pmod{p}$ by assumption, it follows that $x = u_{n+1}$ is a solutions of

$$a_n(x - u_1)\dots(x - u_n) \equiv 0 \pmod{p} \quad (43)$$

This contradicts theorem 1.15.

For (ii), we note that $g(x) \equiv 0 \pmod{p}$ has a degree and that degree is $< n$. By the induction hypothesis, this congruence has fewer than n solutions. This contradicts the earlier observation that this congruence has at least n solutions. Thus the proof is complete.

Corollary 2.27: If $b_n x^n + b_{n-1} x^{n-1} + \dots + b_0 \equiv 0 \pmod{p}$ has more than n solutions, then all the coefficients b_j are divisible by p .

Theorem 2.28:

If $F(x)$ is a function that maps residue classes \pmod{p} to residue classes \pmod{p} ,

then there is a polynomial $f(x)$ with integral coefficients and degree at most $p - 1$ such that $f(x) \equiv F(x) \pmod{p}$ for all residue classes $x \pmod{p}$.

Theorem 3.2: Gauss' Lemma

Let p be an odd prime and $(a, p) = 1$.

$$a, 2a, 3a, \dots, \frac{p-1}{2}a \quad (44)$$

and their least positive residues

Theorem 3.4:

$$\frac{p}{q} \frac{q}{p} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad (45)$$

Note: If p and q are distinct odd primes of the form $4k + 3$, then one of the congruences $x^2 \equiv p \pmod{q}$ or $x^2 \equiv q \pmod{p}$ is a solutions and the other is not. However, if at least one of the primes is of the form $4k + 1$, then both congruences are solvable or both are not.

Proof: Theorem 3.4

Let S be the set of pairs of integers (x, y) such that $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{q-1}{2}$.

The set S has $\frac{(p-1)(q-1)}{4}$ elements. Separate this set into two mutually exclusive subsets S_1 and S_2 according $qx > py$ or $qx < py$. Note that there are no pairs $(x, y) \in S$ such that $qx = py$.

The set S_1 can be described as the set of all pairs (x, y) such that

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{qx}{p} \quad (46)$$

The number of pairs in S_1 is

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p} \right] \quad (47)$$

Similarly for S_2 the number of pairs in S_2 is

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q} \right] \quad (48)$$

Thus we have:

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{qj}{p} \right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{pj}{q} \right] \quad (49)$$

$$= \frac{p-1}{2} \frac{q-1}{2} \quad (50)$$

and hence

$$\frac{p}{q} \frac{q}{p} = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \quad (51)$$

Example: Compute $\left(\frac{42}{61}\right)$

...