Number Theory: Lecture Notes

Anthony Dunford Chris Nash

November 15, 2017

1 Divisibility and Primes

1.1 Introduction

Well ordering Principle:
Let $S \neq 0$ 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 and 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:

$..., b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, ...$

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 $=< r_1 - r < a$ 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 <u>common divisor</u> 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 <u>greatest common divisor</u> of b and c and is denoted by $gcd(b, c)$ or (b, c).

Let $b_1, ..., b_n \in \mathbb{Z}$, not all zero. We denote $g = (b_1, ...b_n)$ 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 $b_1, ..., b_n \in \mathbb{Z}$ not all zero with greatest common divisor g, there exists integers $x_1, ..., x_n$, such that

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

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

Proof: Theorem 1.5

Exercise for the reader.

Theorem 1.6:
For any $m \in \mathbb{Z}, m > 0$

$$(ma, mb) = m(a, b) \tag{2}$$

Proof: Theorem 1.6

By Theorem 1.4 we have:

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

Theorem 1.7:
If $d|a$, $d|b$ and $d > 0$, then

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

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

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

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

$$(a, b) = (b, a) = (a, -b) = (a, b + ax) \tag{5}$$

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

$$
\begin{aligned}
b &= cq_1 + r_1 \quad 0 < r_1 < c && (6)\\
c &= r_1q_2 + r_2 \quad 0 < r_2 < r_1 && (7)\\
r_1 &= r_2q_3 + r_3 \quad 0 < r_3 < r_2 && (8)\\
&... && (9)\\
r_j &= r_{j+1}q_j + r_j \quad 0 < r_j < r_{j-1} && (10)\\
r_{j-1} &= r_jq_{j+1}. && (11)
\end{aligned}
$$

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 $gcd(841, 160)$

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

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

$$
\begin{aligned}
1 &= 37 \times 1 - 4 \times 9 && (13)\\
1 &= 37 \times 1 - (41 - 37) \times 9 && (14)\\
1 &= 37 \times 10 - 41 \times 9 && (15)\\
1 &= (160 - 3 \times 41) \times 10 - 41 \times 9 && (16)\\
1 &= 160 \times 10 - 41 \times 39 && (17)\\
1 &= 160 \times 10 - (841 - 160 \times 5) \times 39 && (18)\\
1 &= (-39) \times 841 + 205 \times 160 && (19)\\
& && (20)
\end{aligned}
$$

Note the solution is not unique:

$$1 = 121 \times 841 - 636 \times 160 \tag{21}$$

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 $a_1, ..., a_n$, all different from zero, have a **common multiple** b if $a_i|b$ for $i = 1, ..., n$. The least of the positive common multiples is called the **least common multiple** and it is denoted by $[a_1, ..., a_n]$ or $lcm(a1, ..., a_n)$

Theorem 1.12:
If b is any common multiple of $a_1, ..., a_n$, then $[a_1, ..., a_n] \mid b$. This is the same as saying that if $h = [a_1, ..., a_n]$ then $0, \pm h, 2 \pm h, ...$ comprise all the common multiples of $a_1, ..., a_n$.

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 probe that $r = 0$. If $r \neq 0$ we argue as follows. For each $i = 1, 2, ..., n$ we know that $a_i|h$ and $a - i|m$, so that $a_i|r$. Thus r is a positive common multiple of $a_1, a_2, ..., a_n$ 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. $[a, b](a, b) = |ab|$

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 allows 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 4b4 and a , cannot be less tahn 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:

$$[a/g, b/g] \cdot (a/g, b/g) = ab/g \tag{23}$$

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, is 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 $p|a_1...a_n$, then p divides at least on 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 Arithmatic
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

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

where k is the unique non-negative integer such that $p^k|n$ but $p^{k+1}|n$
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

$$v_p(mn) = v_p(m) + v_p(n) \tag{25}$$

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 $a \equiv b \ (mod\ m)$

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

Theorem 2.1: Properties of Congruences

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

Theorem 2.2:
Let f denote a polynomial with integral coefficients. If $a \equiv b \ (mod\ m)$ then $f(a) \equiv f(b) \ (mod\ m)$

Theorem 2.3:

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

Definition 2.2:
If $x \equiv y \ (mod\ m)$ then y is called a residue of $x \ (mod\ m)$. A set $x_1, ..., x_m$ is called a complete residue system modulo m if for every integer y, there is one and only one x_j such that $y = x_j \ (mod\ m)$

Theorem 2.4:
If $b \equiv c \ (mod\ m)$, then $(b, m) = (c, m)$.

Definition 2.3:
A reduced residue system modulo m is a set of integers r_i such that
$(r_i, m) = 1,\ r_i \not\equiv r_j,\ (mod\ m)$ 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 obtains 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 reside system 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 $r_1,...,r_n$ be a complete, or a reduced, residue system modulo m. Then $ar_1,...,ar_n$ 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
$a^{p-1} \equiv 1 \ (mod\ p)$. For every integer a,
$a^p \quad \equiv a \ (mod\ p)$.

Theorem 2.8: Euler's Generalization of Fermat's Theorem
If $(a,m)=1$, then

$$a^{\phi}(m) \equiv 1 \ (mod\ m) \tag{26}$$

Theorem 2.9:
If $(a,m)=1$ then there is an x such that $ax \equiv 1 \ (mod\ m)$. Any two such x are congruent $(mod\ m)$. If $(a,m)>1$ then there is no such x.

Lemma 2.10:
Let p be a prime number. Then $x^2 \equiv 1 \ (mod\ p)$ iff $x \equiv \pm 1 \ (mod\ p)$.

Theorem 2.11: Wilson's Theorem
If p is prime, then $(p-1)! \equiv -1 \ (mod\ p)$

Theorem 2.12:
Let p denote a prime. Then $x^2 \equiv -1 \ (mod\ p)$ has solutions iff $p=2$ or $p \equiv 1 \ (mod\ 4)$.

Proof: Theorem

Theorem 2.13:
If p is prime and $p \equiv 1 \ (mod\ 4)$, 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 $q \equiv 3$ (mod 4) then $q|a$ and $q|b$.

Theorem 2.15: (Fermat)
Let

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

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.

$$f(x) = a_n x^n + ... + a_0 \tag{28}$$

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

Definition 2.4:
Let $r_1, ..., r_m$ denote a complete residue system modulo m.
The number of solutions of $f(x) \equiv 0$ (mod m) is the number of the r_i such that $f(r_i) \equiv 0$ (mod m)

Definition 2.5:
Let $f(x) = a_n x^n + ... + a_0$. If $a_n \equiv 0$ (mod m) the degree of the congruence $f(x) \equiv 0$ (mod m) is n. If $a_n \equiv 0$ (mod m), let j be the largest integer such that $a_j \not\equiv 0$ (mod 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 $f(x) \equiv 0$ (mod m), then u is a solution of $f(x) \equiv 0$ (mod d)

- We say that $f(x) \equiv 0$ (mod 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 $f(x) \equiv 0$ (mod m) is an identical congruence
  - e.g. $x^p \equiv x$ (mod 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 $ax \equiv b \ (mod\ m)$ 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 $(mod\ m)$.

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

$$ax \equiv b \ (mod\ n) \tag{29}$$

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

$$ax' + ny' = d \tag{30}$$

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

$$a = da', \quad b = db', \quad n = dn' \tag{31}$$

Dividing (18) by d gives

$$a'x' + n'y' = 1 \tag{32}$$

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

2.3 The Chinese Remainder Theorem

Solve Simultaneous Congruences

Find x (is there are any) that satisfies

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &... \\ x &\equiv a_r \ (mod\ m_r) \end{aligned} \tag{33}$$

Theorem 2.18: The Chinese Remainder Theorem
Let $m_1, ..., m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, ..., a_r \in \mathbb{Z}$. 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 $m - m_1 m_2 ... m_r$

- $m_1, ..., m_r$ positive integers relatively prime in pairs

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

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

- The number of such r-tuples $(a_1, ..., a_r)$ is $m = m_1 m_2 ... m_r$.
- 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 $(a_1, ..., a_r) \neq (a'_1, ..., a'_r)$. then $a_i \neq a'_i$ for some i, and we see that no integer x satisfies both the congruences $x \equiv a_i\ (mod\ m_i)$ and $x \equiv a'_i\ (mod\ m_i)$
- This we have a one-to-one correspondence between the r-tuples $(a_1, ..., a_r)$ and a complete residue system modulo m, such as the integers $1, ..., m$

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 $m = \Pi p^\alpha$ then

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

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 $f(x) \equiv 0\ (mod\ m)$. 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 $N(m) = \prod N(p^a lpha)$

2.4 Public-key Cryptography

Lemma 2.22:
Suppose $m \in \mathbb{Z},\ m > 0,\ (a, m) = 1$. If $k, \overline{k}\mathbb{Z}$ and $k, \overline{k} > 0$ such that $k, \overline{k} \equiv 1\ (mod\ \phi(m))$, then $a^{k\overline{k}} \equiv a\ (mod\ m)$.

Proof: Theorem 2.22
Write $k\overline{k} = 1 + r\phi(m)$ for some $r \in \mathbb{Z}$. Then by Euler's congruence

$$a^{k\overline{k}} = aa^{r\phi(m)} = a(a^{\phi(m)})^r \equiv a \cdot 1^r = a\ (mod\ m)$$

- If $(a,m)=1,\ k>0$, then $(a^k,m)=1$. Thus if $n=\phi(m)$ and $r_1,...,r_n$ is a system of reduced residues $(mod\ m)$, then the numbers $r_1^k,...,r_n^k$ are also relatively prime to m. These k^{th} powers may not all be distinct $(mod\ m)$, 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 $(mod\ m)$ provided that $(k,\phi(m))=1$.

- Suppose that $r_i^k \equiv r_j^k\ (mod\ m)$ and $(k,\phi(m))=1$. By theorem 2.9 we may find $\overline{k}>0$ such that $k\overline{k}\equiv 1\ (mod\ \phi m)$ and then it follows from the lemma that

$$r_i \equiv r_i^{k\overline{k}} = (r_i^k)^{\overline{k}} \equiv (r_j^k)^{\overline{k}} = r_j^{k\overline{k}} \equiv r_j\ (mod\ m) \tag{36}$$

  This implies that $i=j$. We will show later that the converse also holds: the numbers $r_i^k,...,r_n^k$ are distinct $(mod\ m)$ only if $(k,\phi(m))=1$. Suppose that $(k,\phi(m))=1$. Since the numbers $r_1,...,r_n^k$ are distinct $(mod\ m)$, they form a system of reduced residues $(mod\ m)$. That is the map $a\mapsto a^k$ permutates the reduced residues $(mos\ m)$ if $(k,\phi(m))=1$. The significance of the lemma is that the further map $b\mapsto b^{\overline{k}}$ 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 $m=p_1p_2$ 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 genuis!'*. The associate first converts the characters to number in some standard way, say by emplying (ASCII). Then $G=071$, $a=097$,..., $!=033$. Then concatenate these codes to form a number

    $a=071097117115115126119097115126097126103101110105117115033$
  - if the message were longer, it could be ficided 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, $0\le b<m$ such that $b\equiv a^k\ (mod\ m)$ and sends this b to us.
  - We use Euclidean Algorithm to find $\overline{k}>0$ such that $k\overline{k}\equiv 1\ (mod\ \phi(m))$ and then we find the unique c such that $0\le c<m$, $c\equiv b^{\overline{k}}\ (mod\ m)$. 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 $\overline{k}$. 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 $f(x) \equiv 0\ (mod\ m)$. Suppose that $m = m_1 m_2$, where $(m_1, m_2) =$. With a "little work", theorem 2.19 shows that the roots of the congruence $f(x) \equiv 0\ (mod\ m)$ are in one-to-one correspondence with pairs (a_1, a_2) in whic a_1 runs over all roots of the congruences $f(x) \equiv 0\ (mod\ m_1 andin)$ a_2 runs over all roots of the congruence $f(x) \equiv 0\ (mod\ m_2)$.

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

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

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

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

  Suppose that $x = a$ is a solution of $f(x) \equiv 0\ (mod\ p^j)$ 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

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

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

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

  as the following argument shows. What we want to establish is that the coefficients of $t^1, t^3, ..., t^n$ in (37) are divisible by p^{j+1} and so can be ommited 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, $2 \le k \le n$. To see this, let cx^r be a representative term from $f(x)$. The corresponding term in $f^{(k)}(a)$ is $cr(r-1)(r-2)...(r-k+1)a^{r-k}$.

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 $t^2, t^3, ..., t^n$ 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 $f(x) \equiv 0 \ (mod\ p^{j+1})$. We want t to be a solution of

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

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

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

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

Theorem 2.3: Hansel's Lemma:
Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \ (mod\ p^j)$ and $f'(a) \not\equiv 0 \ (mod\ p)$ then there is a unique $t \ (mod\ p)$ such that $f(a + tp^j) \equiv 0 \ (mod\ p^{j+1})$

- If $f(a) \equiv 0 \ (mod\ p^j)$, $f(b) \equiv 0 \ (mod\ p^k)$, $j < k$ and $a \equiv b \ (mod\ p^j)$, then we say that <u>b lies above a</u>, or <u>a lifts to b</u>.
- If $a \equiv b \ (mod\ p^j)$, then a is called a <u>nonsingular</u> root if $f'(a) \not\equiv 0 \ (mod\ p)$; otherwise it is <u>singular</u>.
- By Hensel's lemma we see that a nonsingular root $a \ (mod\ p)$ lifts to a unique root $a_2 \ (mod\ p^2)$. Since $a_2 \equiv a \ (mod\ p)$ it follows by theorem 2.2 that $f'(a_2) \equiv f'(a) \not\equiv 0 \ (mod\ p)$. 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 uniques root a_j modulo p^j ofr $j = 2, 3, ...$ by (2.5) we see that this sequence is generated bby means of the recursion

$$a_{j+1} = a_j - f(a_j)\overline{f'(a)} \tag{40}$$

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

Example: Solve $x^2 + x + 47 \equiv 0 \ (mod\ 7^3)$

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

- $f'(1) = 3 \equiv 0 \ (mod \ 7)$
- $f'(5) = 11 \equiv 0 \ (mod \ 7)$

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

2.6 Prime Modulus

$f(x) \equiv 0 \ (mod \ m) \rightarrow f(x) \equiv 0 \ (mod \ p)$ *(reduced)*

Theorem 3.2: Gauss' Lemma
Let p be an odd prime and $(a, p) = 1$.

$$a, 2a, 3a, ..., \frac{p-1}{2}a \tag{41}$$

and their least positive residues