math115A lecture notes

Alice Bob

Table of Contents

0.1. January 7

Basic Properties : What questions are studied in this subject?

0.1.1. Remark

Fermat (1636): Every positive integer can be represented as a sum of the squares of four integers
e.g. $1 = 1^2 + 0^2 + 0^2 + 0^2$
e.g. $7 = 2^2 + 1^2 + 1^2 + 1^2$
e.g. $10 = 2^2 + 2^2 + 1^2 + 1^2$

Langrange published the first proof in 1770

0.1.2. Definition: prime number

A positive integer p is prime if its only positive divisors are 1 and p. (should be greater than 1)

0.1.3. Remark

Euclid proved that there are inifinitely many primes

0.1.4. Remark

Fermat: All numbers of the form $f_n := 2^{2^n} + 1$ are prime.
Therefore, for example, $641 \mid 2^{2^5} + 1$ (check this)

0.1.5. Remark

Gauss: A regular polygon with m sides can be constructed as using straight edge and compasses alone iff $m = 2^k \cdot f_{n_1} \cdot f_{n_2} \cdot \ldots \cdot f_{n_r}$ (check this)

0.1.6. Remark

How are the primes distributed?

$\pi(x) = |\{n \leq x : \text{n is prime}\}|$

How does $\pi(x)$ grow with x?

Gauss used tables of primes to guess the answer e.g. look at values $\frac{\pi(x) - \pi(x - 1000)}{1000}$ for large x i.e. frequency of primes in [x - 1000, x]

He noticed that this frequency call it $\Delta(x)$ seems to be slowly decreasing. He then noticed that $\frac{1}{\Delta(x)} \cong \frac{1}{\log(x)}$ (for log base e) so that $\pi(x) \approx \int_2^x \frac{\mathrm{d}t}{\log t}$

Then, if we define $\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}$ then the following conjecture was made:

$$\lim_{x \to \infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1$$

And later proved by Hadamard using complex variable theory

0.2. Properties of $\mathbb{Z}$

0.2.1. ***Proposition***

properties of $\mathbb{Z}$
1. cancellation law: if ab = ac then b = c as long as $a \neq 0$ ($\mathbb{Z}$ is said to be a domain or an integral domain)
2. $\mathbb{Z}$ is ordered therefore $\mathbb{Z}^+$ is closed under addition and multiplication and for every $a \neq 0$ exactly one of a, -a belongs to $\mathbb{Z}^+$. Define $a > b$ to mean $a - b \in \mathbb{Z}^+$
3. $\mathbb{Z}^+$ is well ordered: Every non-empty set of positive integers has a smallest element. (note that $\mathbb{Q}, \mathbb{R}$ are NOT well-ordered)

0.2.2. Remark

We can partiion the integers into three classes:

1. Units ± 1 (i.e. integers with reciprocals in $\mathbb{Z}$)
2. Prime numbers (i.e. integers n for which we cannot have $n = ab$ with $a, b \in \mathbb{Z}$ and a, b not units)
3. Composite numbers (the rest)

0.2.3. Definition: If m, n are integers, we say that m divides n (written $m \mid n$) if there exists an integer t such that $n = mt$. Otherwise write $m\ |!n$

0.3. Types of proofs:

0.3.1. ***Theorem***

Every integer $n > 1$ is divisible by a positive prime.

Proof

Suppose that $n > 1$ has no positive prime divisor. Then n is not prime, and we may write $n = ab$, with a and b not units. Then $n = |a| \cdot |b|$ and $|a| < n$ since $|b| > 1$.

Set $n_1 = |a|$. Then $n_1 > 1$ and n_1 has no prime divisor

Now repeat the above argument with n_1 in place of n to produce an integer n_2 with $1 < n_2 < n_1$ and such that n_2 has no prime divisor. Continuing in this way, we produce a non-empty set of positive integers $n_1, n_2, \ldots$ having no smallest integer.

However, this contradicts the well-ordering principle.

$\square$

0.3.2. ***Theorem***

> There are infinitely many positive primes

Proof

Suppose that there are only finitely many positive primes.

Consider the integer $N = p_1 ... p_2 ... p_r + 1$. Then p_i does not divide N for all i, but $N > 1$ and our previous result shows that N is divisible by some prime. Henve there is a prime p distinct from $p_1, ..., p_r$ such that p divides N. (this leads to a contradiction)

$\square$

no class next tuesday yay

0.3.3. ***Theorem***

> There is no integer between 0 and 1

Proof

Suppose that there exists $m \in \mathbb{Z}$ such that $0 < m < 1$. Then we have

$$\begin{gathered} 0 < m^2 < m < 1 \Rightarrow \\ 0 < m^3 < m^2 < m < 1 \Rightarrow \\ 0 < m^4 < m^3 < ... \end{gathered}$$

and so we obtain an infinite set of positive integers with no smallest element. This contradicts the well-ordering principle.

$\square$

0.3.4. ***Theorem***

> The real number e is irrational

Proof

We know that $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots$.

So for each $n \in \mathbb{Z}^{+}$, we have $n!e = \frac{n!}{1} + \frac{n!}{2} + \dots + \frac{n!}{n!} + \frac{n!}{(n+1)!} + \dots$

Suppose that e were irrational then $e = \frac{a}{b}$, with $a, b \in \mathbb{Z}$. If this is true, then

$n!\frac{a}{b} = q_n + \frac{n!}{(n+1)!} + \dots$

set $r_n := n!a - q_n b$

$r_n = n!a - q_n b = b\left(\frac{n!}{(n+1)!} + \frac{n!}{(n+2)!}\right)$

Since $r_n \in \mathbb{Z}$ we have $r_n < \frac{b}{n+1} + b\left(\frac{1}{(n+1)(n+2)} + \frac{1}{(n+2)(n+3)} + \dots\right) = \frac{b}{n+1} + b\left(\left(\frac{1}{n+1} - \frac{1}{n+2}\right) + \left(\frac{1}{n+2} - \frac{1}{n+3}\right) + \dots\right) = \frac{b}{n+1} + \frac{b}{n+1} = 2\frac{b}{n+1}$

Hence if $n \geq 2b$ we have $0 < r_n < 2\frac{b}{n+1} < 1$ which is a contradiction by the previous theorem (hence e is irrational)

$\square$

0.3.5. ***Theorem:*** **Principle of Induction**

> If a set S of integers contain n_0, and if S contains $n + 1$ whenever it contains n, then S contains all integers greater than or equal to n_0

Proof

Suppose that m is an integer with $m > n_0$, and $m \notin S$. Then $m - 1 \notin S$ for otherwise, since $m = (m - 1) + 1$ we would have $m \in S$

Hence $m - 1 \neq n_0$ therefore $m - 1 > n_0$. Now we can continue to repeat the argument and thereby obtain a contradiction to the well ordering principle

$\square$

0.3.6. ***Theorem:*** **Birrchlet's pigeonhole principle**

> suppose that a set of n elements is partitioned with m subsets with $1 \leq m < n$. Then some subset must contain more than one of the elements.

0.4. Back to number theory

0.4.1. ***Proposition***

> Every natural number greater than 1 is either a prime or can be written as a product of primes.

Proof

Proof via induction :

Let $n \in \mathbb{Z}^{+}$. If n is prime, then there is nothing to prove.

However if n is composite we can write $n = ab$ with $0 < a, b < n$. By induction a and b are either primes or expressible as a product of primes, and so substituting for n yields an expression for n as a product of primes.

$\square$

0.4.2. ***Theorem:*** **Fundamental theorem of arithmetic**

> Any natural number greater than 1 can be represented in one and only one way as a product of primes

Proof

Let $P(n)$ denote the statement "n can be written uniquely as a product of primes"

observe that 2 is prime, so that $P(2)$ is true.

Suppose for inductive hypothesis that k is an integer such that $P(t)$ is true for all integers t satisfying $2 \leq t \leq k$

Consider $k + 1$. If this is prime, then we are trivially done.

Suppose $k + 1$ is composite (so that it has at least 2 prime factors) and (for contradiction) has 2 distinct representations as products of primes:
$k + 1 = pqr... = p'q'r'...$

(Note that the same prime cannot be in both representations (as P(t) is true for all $2 \leq t \leq k$))

Suppose WLOG that p and p' are the smallest primes occuring in each factorization

Since $k + 1$ is composite, we have $k + 1 \geq p^2$ and $k + 1 \geq p'^2$ and since $p \neq p'$ then at least one of these ineuqalities is a strict inequality, therefore $k + 1 > pp'$

Consider $k + 1 - pp'$ which by induction hypothesis can be written uniquely as a product of primes. Since this quantity is divisible by both p and p', we have the prime factorization $k + 1 - pp' = pp'QR...$ implies pp' divides $k + 1$, this implies that ...

$\square$

0.4.3. Remark

Consequences of Fundamental theorem of arithmetic.

suppose that the prime factorisation of $n \in \mathbb{Z}^+$ is given by $n = p_1^{q_1} p_2^{q_2} ... p_r^{q_r}$ with $p_1, ..., p_2$ distinct primes. The divisors of n consist of all products of the form $p_1^{\alpha_1} ... p_r^{\alpha_r}$ where $0 \leq \alpha_i \leq q_i$ and the total number of choices is $(\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_r + 1) = \prod_{i=1}^{r} (\alpha_i + 1)$

let $d(n)$ be the number of divisors of n

We may consider the sum $\sigma(n)$ of all divisors of n (including 1 and n). We have that $\sigma(n) = (1 + p_1 + p_1^2 + ... + p_1^{q_1})(1 + p_2 + p_2^2 ... p_2^{q_2})...(1 + p_r + p_3^r + ... + p_1^{q_r})$

when we multiply this expression it is the sum of all possible products of the sum $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$

(this is probably in the book)

0.5. January 16

0.5.1. Definition

A positive number n is said to be perfect if the sum of the divisors of n including 1 and excluding n is equal to n

0.5.2. *Theorem:* (by Euclid)

> Suppose that p is a prime such that $p + 1 = 2^k$ for some $k > 0$. Then $2^{k-1} \cdot p$ is pefect.

Proof

Took a picture

□

0.5.3. *Theorem:* (Euler)

> Every even perfect numbers is of the form $2^{k-1} \cdot p$, where $p + 1 = 2^k$

Proof

Did not do in class

□

0.5.4. Remark

are there any odd perfect numbers (open question)

0.5.5. ***Proposition***

> If m, n have common prime factors, we may obtain the greatest common divisor or highest common factor (HCF) of m and n by multiplying together the various common prime factors of m and n, each of these being taken to the highest power to which it divides both m and n

Proof

For example, $3132 = 2^2 \cdot 3^3 \cdot 29$ and $7200 = 2^5 \cdot 3^2 \cdot 5^2$ then the highest common factor is $2^2 \cdot 3^2 = 36$

$\square$

0.5.6. ***Theorem:*** **division theorem**

> If a is any integer and $b \in \mathbb{Z}^+$, then there exists exactly one pair of integers q and r such that the condition $a = bq + r$ where $0 \leq r < b$ hold. (the number q is called the quotient and r is the remainder when a is divided by b)

Proof

look it up

$\square$

0.5.7. Algorithm: Euclid's algorithm

Finds the highest common factor of two positive integers a and b. Suppose that $a > b$. Then

$$a = qb + c, 0 \leq c < b$$

Any common divisor of a and b is also a common divisor of b and c. So we've reduced the problem to finding the highest comon factor of b and c (which are respectively less than and b).

i.e. the problem we are solving is $b = rc + d, 0 \leq d < c$

The common divisors of b and c are the same as those of c and d. etc.

We can repeat this process until we arrive at a number which is a divisor of the preceding number.

0.5.8. Definition

Suppose that $a, b \in \mathbb{Z}^+$. Say that $n \in \mathbb{Z}$ is linearly dependent on a and b if it can be written in the form $n = ax - by$ for some $x, y \in \mathbb{Z}^+$.

Remarks:

(i) Any number representable in the form $ax - by$ can also be represented in the form $by' - ax'$ with $x', y' \in \mathbb{Z}^+ \cup \{0\}$

Observe that $ax - by = by' - ax' \Leftrightarrow a(x + x') = b(y + y')$. To ensure that this last equality holds, take any integer m such that $mb > x$ and $ma > y$.

Then define x' and y' by $x + x' = mb, y + y' = ma$.

(ii) If n is linearly dependent on a and b, then so is kn for any integer k

(iii) If n_1, n_2 are (both)linearly dependent on a, b then so is $n_1 + n_2$

We come to an interesting property of the HCF:

0.5.9. ***Theorem***

The HCF h of two positive integers a and b is representable in the form $h = ax - by$ where $x, y \in \mathbb{N}$

Proof

Consider the stpes involved in Euclid's algorithm. Observe that a, b are linearly dependent on a, b since $a = a(b + 1) - ba, b = ab - b(a - 1)$.

Now we have $a = qb + c$. So, since b is linearly dep on a,b so is q^b. Hence $c = a - qb$ is linearly dependent on a, b. Continue in this way to deduce that the last remainder is the applicatino of the algorithm, i.e. h is linearly dependent on a,b.

Example: took a picture (this seems important)

$\square$

0.5.10. Remark

Here is a problem: suppose that $a, b \in \mathbb{Z}_{\geq 0}$. Find $x, y \in \mathbb{Z}$ such that $ax + by = n$ (†)
This is an example of a Diophantine Euqation (it does not determine x, y uniquely.)

Remakrs:

1. Note that (†) cannot be solved unless n is a multiple of the HCF h of a, b since $h \mid (ax + by)$
2. Suppose that $n = mh$. Then † can be solved. First solve $ax_1 + by_1 = h$. We've already seen: set $x = mx_1$ and $y = my_1$

0.6. January 21

Last time: diophantine equations

0.6.1. Remark

Solving Diophantine Equations:

Suppose that $a, b, n \in \mathbb{Z}_{\geq 0}$. Find $x, y \in \mathbb{Z}$ such that $ax + by = n$ (†)

Remarks:

1. (†) cannot be solved unless n is a multiple of $h := \operatorname{gcf}(a, b)$, since $h \mid (ax + by)$
2. Suppose that $n = mh$ Then (†) can always be solved.

First, solve $ax_1 + by_1 = h$

Then set $x = mx_1, y = my_1$

In fact, (†) is solvable with $x, y \in \mathbb{Z}$ if and only iff n is a multiple of h. So, if $h = 1$ then (†) is solvable for all $n \in \mathbb{N}$ (and also for $n \in \mathbb{Z}$).

3. Suppose that $h = 1$ and that $(x, y), (x', y')$ are two distinct solutions of (†) . Then $a(x - x') + b(y - y') = n - n = 0$.
   Therefore $\frac{a}{b} = \frac{-y(y-y')}{x-x'}$

Since a, b are coprime there exists $t \in \mathbb{Z}$ such that $y - y' = -at$ and $x - x' = bt$

Additionally, any integers of the form $y = y' - at$ and $x = x' + bt$ satisfy (†)

So if $h = 1$ then a general solution of (†) is $x = x' + bt, y = y' - at$

4. Now suppose that $h > 1$, and $n = mh$ so (†) has a solution. Then $ax + by = n = mh \Leftrightarrow \frac{a}{h}x + \frac{b}{h}y = m$. Since the HCF of $\frac{a}{h}, \frac{b}{h}$ is 1, we've already dealt with this case: the general solution is $x = x_0 + \frac{b}{h}t, y = y_0 - \left(\frac{a}{h}\right)t$ $(t \in \mathbb{Z})$ where x_0, y_0 is a solution of (†)

0.6.2. Example: : Solve two variable diophantine equation

Find the general solution of $69x + 39y = 15$ (if it exists)

First determine if the equation is solvable: find the HCF of 69,39:

69 = 39 times 1 + 30
39 = 30 times 1 + 9
30 = 9 times 3 + 3
9 = 3 times 3
Therefore the equation is solvable, since $3 \mid 15$

Next: $\frac{69}{3}x + \frac{39}{3}y = 15 \Leftrightarrow 23x + 13y = 5$

From the Euclidean algorithm, we obtain $3 = 30 - 9 \times 3 = 4(69 - 39 \times 1) - 3 \times 39 = 4 \times 69 - 7 \times 39$. Therefore $x = 4, y = -7$ is a solution of $69x + 39y = 3$ and $23x + 13y = 1$.

Then, $x_0 = 4 \times 5, y_0 = -7 \times 5$ is a solution of $69x + 39y = 15$

And a general solution of (†) is $x = 20 + 13t, y = -35 - 23t$

0.6.3. Chatper 2 Congruences

0.6.4. Definition: Congruent modulo m

Suppose that $a, b \in \mathbb{Z}$. We say that a is congruent to b modulo m and write $a \equiv b (\operatorname{mod} m)$ or $a \equiv b(m)$ (Informally, "equality except for the addition of some multiple of m")

Examples: $63 \equiv 0 \operatorname{mod} 3, 7 \equiv -1 \operatorname{mod} 8, 5^2 \equiv -1 \operatorname{mod} 13$

Additionally, note that $x \equiv y \operatorname{mod} 2 \Leftrightarrow$ x and y are both even or x and y are both odd

0.6.5. Remark

If $a \equiv \alpha, b \equiv \beta \operatorname{mod} m$ then

$$\begin{aligned} a + b &\equiv \alpha + \beta \operatorname{mod} m, \\ a - b &\equiv \alpha - \beta \operatorname{mod} m, \\ ab &\equiv \alpha\beta \operatorname{mod} m \end{aligned}$$

Proof:

Since $a \equiv \alpha \operatorname{mod} m$ and $b \equiv \beta \operatorname{mod} m$ it follows that $a = \alpha + k_1 m, b = \beta + k_2 m$ for some integers k_1, k_2 hence $a + b = \alpha + k_1 m + \beta + k_2 m = \alpha + \beta + m(k_1 + k_2)$. Therefore $(a + b) - (\alpha - \beta)$ is divisible by m, and so $a + b \equiv \alpha + \beta \operatorname{mod} m$ $\square$

0.6.6. Remark

If $a = \alpha m$, then $ka \equiv k\alpha m$ for any $k \in \mathbb{Z}$

0.6.7. Remark

It is true that $42 \equiv 12 \operatorname{mod} 10$ however $\frac{42}{6} \not\equiv \frac{12}{6} \operatorname{mod} 10$

However, we CAN cancel factors if they are coprime to the modulus.

i.e. suppose that $ax \equiv ay \operatorname{mod} m$ with a, m coprime then $m \mid a(x - y)$ and this implies $m \mid (x - y)$ i.e. $x \equiv y \operatorname{mod} m$

0.6.8. Remark

Suppose that $n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10 + a_0$.
Observe that $n \equiv a_0 \bmod 2$. Therefore n is divisible by 2 if and only if a_0 (the last digit of n) is divisible by 2

Next, notice that $10 \equiv 1 \bmod 3$. Therefore $n \equiv a_m + a_{m-1} + \ldots + a_1 + a_0 \bmod 3$. In other words, the sum of the digits of n is divisible by 3 if and only if n is divisible by 3.

Observe that $10 \equiv 0 \bmod 5$ and so $n \equiv a_0 \bmod 5$. Therefore $n \equiv 0 \bmod 5$ iff $a_0 \equiv 0 \bmod 5$ (i.e. n is divisible by 5 if and only if the last digit of n is divisible by 5)

Observe that $10 \equiv 1 \bmod 9$ (similar to 3, n is divisible by 9 iff the sum of its digits is divisble by 9)

Observe that $10 \equiv -1 \bmod 11$. Hence $n \equiv a_m \cdot (-1)^m + a_{m-1} \cdot (-1)^{m-1} + \ldots + a_1 \cdot (-1) + a_0$. (i.e. n is divisble by 11 if and only if the alternating sum of the digits of n is divisible by 11)

0.6.9. Remark

Notice that $7 \cdot 11 \cdot 13 = 10^3 + 1$

Any integer is congruent modulo m to exactly one of the numbers $\{0, 1, 2, \ldots, m-1\}$. This set of numbers is called a complete set of residues modulo m.

0.6.10. Remark

"Congruence modulo m" is an equivalence relation on $\mathbb{Z}$

0.7. January 23

Notation: If $a, b \in \mathbb{Z}$ then we write (a, b) for the HCF of a and b

0.7.1. Definition: Linear Congruences

A linear congruence is of the form $ax \equiv b (\operatorname{mod} m)$ (†)

0.7.2. *Theorem*

> The congruence (†) can be solved if and only if $(a, m) \mid b$

Proof

Since $(a, m) \mid a$ and $(a, m) \mid m$ it foolows that if (†) is solvable, then we must have $(a, m) \mid b$

For the converse, set $d = (a, m)$, and suupose that $d \mid b$. Let $a' = \frac{a}{d}, b' = \frac{b}{d}, m' = \frac{m}{d}$

Then to solve † it suffices to solve $a'x \equiv b' (\operatorname{mod} m')$(††)

Now (due to properties of gcf) we have $(a', m') = 1$, and as x runs through a complete set of residues $\operatorname{mod} m'$, so does $a'x$ (since there are m' of these numbers, no two of which are congruent modulo m')

Hence (††) has precisely one solution modulo m'

If y is any solution of $a'x \equiv b' (\operatorname{mod} m')$, then the complete set of solutions modulo m of (†) is given by $x = y, x = y + m', x = y + 2m', ..., x = y + (d - 1)m'$

□

0.7.3. Example

Consider $3x \equiv 5 (\operatorname{mod} 11)$

A complete set of residues mod 11 is $\{0, 1, 2, ..., 10\}$

Another complete set of residuces is $\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$ mod 11

and these are congruent modulo 11 respectively to $0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8$ respectively.
The value 5 occurs when $x = 9$

0.7.4. Example

Complete set of residues of 6 is $\{0, 1, 2, 3, 4, 5\}$

If we multiply this set with something coprime to 6 then $\{0, 5, 10, 15, 20, 25\}$ is still complete set of residues

However if we multiply by something that is not coprime to 6, such as 2, then the set $\{0, 2, 4, 6, 8, 10\}$ is not a complete set of residues as they are confruent to $\{0, 2, 4, 0, 2, 4\}$ (mod 6)

recall that $ax \equiv ay (\operatorname{mod} m)$, a can be canceld iff $(a, m) = 1$ (from 1.6.7)

0.7.5. *Corollary*

> The above implies that $ax \equiv b (\operatorname{mod} p)$ is solvable where p is prime.

0.7.6. Remark

The congruence $ax \equiv b (\bmod m)$ is equivalent to the equation $ax = b + my$ i.e. $ax - my = b$. We have seen that this diophantine equation can be solved if any only if b is a multiple of (a, m)

0.7.7. *Theorem:* Chinese Remainder

> Suppose that $n_1, ..., n_k \in \mathbb{Z}^+$ and that $(n_i, n_j) = 1$ for $i \neq j$ (i.e. pairwise coprime)
> Then, for any $c_1, ..., c_k \in \mathbb{Z}$ there is an integer x satisfying $x \equiv c_j (\bmod n_j), 1 \leq j \leq k$ (†)

Proof

Let $n = n_1 \cdot n_2 ... n_k$ and set $m_j = \frac{n}{n_j}$ for $(1 \leq j \leq k)$. Then $(m_j, n_j) = 1$ and so there exists an integer x_j such that $m_j x_j \equiv c_j (\bmod n_j)$(†)
The integer $x = m_1 x_1 + ... + m_k x_k$ satisfies $x \equiv c_j (\bmod n_j)$

□

0.7.8. Remark

Let $x = m_1 x_1 + ... m_2 x_2 + ... + m_k x_k$

Consider x mod n_2. We have $x \equiv 0 + m_2 x_2 + 0 + 0 + ... + 0 (\bmod n_2) \equiv c_2 (\bmod n_2)$

0.7.9. Remark

Infact, there is a unique solution to the congruence (†) modulo $n = n_1 ... n_k$.

Proof: suppose that x, y are solutions to (†) Then we have $x \equiv y (\bmod n_j)$ i.e. $x - y \equiv 0 (\bmod n_j)$.

Since the integers n_j are pairwise coprime, this implies that $x - y \equiv 0 (\bmod n)$ i.e. $x \equiv y \bmod (n)$

0.7.10. Example

Consider $x \equiv 2 (\bmod 5), x \equiv 3 (\bmod 7), x \equiv 4 (\bmod 11)$.

Therefore $n_1 = 5, n_2, = 7, n_3 = 11$ and $n = 5 \cdot 7 \cdot 11$ so that $m_1 = 77, m_2 = 55, m_3 = 35$
Hence we must solve: $77 x_1 \equiv 2 (\bmod 5), 55 x_2 \equiv 3 (\bmod 7), 35 x_3 \equiv 4 (\bmod 11)$

Which can be simplified to $2 x_1 \equiv 2 (\bmod 5), 6 x_2 \equiv 3 (\bmod 7), 2 x_3 \equiv 4 (\bmod 11)$

A solution is given by $x = 77 x_1 + 55 x_2 + 35 x_3$ and we can take $x_1 = 1, x_2 = 4, x_3 = 2$ which give $x = 367$

0.7.11. Definition: Order of x

Suppose that $m \in \mathbb{Z}^+$ and $x \in \mathbb{Z}$ with $(m, x) = 1$. The order of $x (\mathrm{mod}\, m)$ is the smallest positive integer l satisfying $x^l \equiv 1 (\mathrm{mod}\, m)$

0.7.12. Example

the powers of $3 \bmod 11$ are $3, 9, 5, 4, 1, 3, 9, \ldots$. Then the order of $3 \bmod 11$ is 5

0.7.13. *Proposition*

$x^n \equiv 1 \,\mathrm{mod} (m) \Leftrightarrow n$ is a multiple of l. Where l is the order of $x \bmod m$.

Proof

We have $n = ql + r, 0 \leq r \leq l - 1$. Therefore $x^n = x^{ql} \cdot x^r$ = x^r . We have that $x^r = 1$ iff $r = 0$

□

0.7.14. *Theorem:* Fremat's Little Theorem

Suppose that $m \in Z^+$ and let $x \in \mathbb{Z}$ with $(m, x) = 1$. Consider the sequence $x, x^2, x^3, \ldots$

Then there exist k, h with $x^k \equiv x^h (\mathrm{mod}\, m)$.

Since $(x, m) = 1$ this implies that $x^{h-k} \equiv 1 (\mathrm{mod}\, m)$

0.8. January 28

We finish Fermat's Little Theorem:

0.8.1. Definition: Fermat's Little Theorem

Suppose that $m \in \mathbb{Z}^+$ and $x \in \mathbb{Z}$ with $(m, x) = 1$. The order of $x \bmod m$ is the smallest positive integer l satisfying $x^l \equiv 1 (\mathrm{mod}\, m)$

0.8.2. *Proposition*

We have that $x^n \equiv 1 (\mathrm{mod}\, m)$ if and only if n is a multiple of l

0.8.3. Remark

Suppose that p is a prime number. Let $1 \leq r \leq p-1$ be an integer. Recall that $\binom{p}{r} = \frac{p!}{(p-r)!r!}$

We therefore see that $p \mid \binom{p}{r}$ i.e. $\binom{p}{r} \equiv 0 (\operatorname{mod} p)$

Now suppose that x, y are intleterninates. Then

$$(x+y)^p = \binom{p}{1} x^{p-1} y + \cdot + \binom{p}{1} x^{p \cdot r} y^r + \ldots + p x y^{p-1} + y^p$$

$$\equiv x^p + y^p (\operatorname{mod} p)$$

Hence one can show by induction that $(x_1 + x_2 + \ldots + x_n \equiv x_1^p + x_2^p + \ldots + x_n^p (\operatorname{mod} p))$

0.8.4. ***Theorem:*** **Fermat's Little Theorem**

> Suppose that p is a prime number and that $x \not\equiv 0 (\operatorname{mod} p)$. Then $x^{p-1} \equiv 1 (\operatorname{mod} p)$

Proof

We have $x = 1 + 1 + \ldots + 1$ (x times) therefore $x^p = (1 + 1 + \ldots + 1)^p \equiv 1^p + 1^p + \ldots + 1^p (\operatorname{mod} p) \equiv x (\operatorname{mod} p)$. Since $(x, p) = 1$ this implies that $x^{p-1} \equiv 1 (\operatorname{mod} p)$

Second proof: Consider the numbers $x, 2x, 3x, \ldots, (p-1)x$. There are $p-1$ numbers in this set and no two fo them are congruent modulo p. Here this set forms a complete set of non-zero residues modulo p, and are congruent (in some order) to $1, 2, 3, \ldots, p-1$

Therefore $x \cdot 2x \cdot 3x \ldots (p-1)x \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) (\operatorname{mod} p)$ i.e. $x^{p-1} \cdot (p-1)! \equiv (p-1)! (\operatorname{mod} p)$

Since $(p, (p-1)!) = 1$, it foolows that $x^{p-1} \equiv 1 (\operatorname{mod} p)$

$\square$

0.8.5. Definition: Euler ϕ function

Suppose that $m \in \mathbb{Z}^+$. Then $\phi(m)$ is defined to be the number of elements in the set $1, 2, \ldots, m-1$ that are coprime to m.

Example: suppose that p is a prime. then $\phi(p) = p - 1$

0.8.6. *Theorem:* Euler's

> Suppose that $m \in \mathbb{Z}^+$ and that $(x, m) = 1$. Then $x^{\phi(m)} \equiv 1$

Proof

Let $\alpha_1, \alpha_2, ..., \alpha_{\phi(m)}$ denote the elements of the set $\{1, 2, ..., m - 1\}$ that are coprime to m.

Then the numbers $x \cdot \alpha_1, ..., x \cdot \alpha_{\phi(m)}$ are congruent (in some order) to the numbers $\alpha_1, ..., \alpha_{\phi(m)}$

In other words $x\alpha_1 ... x\alpha_{\phi(m)} \equiv \alpha_1 ... \alpha_{\phi(m)} (\operatorname{mod} m)$

i.e. $x^{\phi(m)} \cdot \alpha_1 ... \alpha_{\phi(m)} \equiv \alpha_1 ... \alpha_{\phi(m)} (\operatorname{mod} m)$. Hence $x^{\phi(m)} \equiv 1 (\operatorname{mod} m)$.

□

0.8.7. Example

Take $m = 20$, the positive integers less than 20 and corpime to 20 are $1, 3, 7, 9, 11, 13, 17, 19$ Therefore $\phi(m) = 8$. Note that if we multiply this set of numbers of 3 then none of the new numbers will be congruent to 20. i.e. the residues would be $3, 9, 1, 7, 13, 19, 11, 17 (\operatorname{mod} 20)$.

We have $3^8 \equiv 1 (\operatorname{mod} 20)$ and (note that $3^8 = 6561$)

0.8.8. *Theorem:* Wilson's Theofrem

> If p is a prime, then $(p - 1)! \equiv 1 (\operatorname{mod} p)$

Proof

Suppose that $p > 3$. (the cases $p = 2, 3$ are clear.)

Consider the set of integers $S = \{1, 2, 3, ..., p - 1\}$

For each $a \in S$ there exists a unique $a' \in S$ such that $aa' \equiv 1 (\operatorname{mod} p)$

If $a = a'$ then we have $a^2 \equiv 1 (\operatorname{mod} p)$ if and only if $a^2 - 1 \equiv 0 (\operatorname{mod} p)$ if and only if $(a - 1)(a + 1)(\operatorname{mod} p) \equiv 0$ if and only if $a - 1 \equiv 0 (\operatorname{mod} p) \Rightarrow a \equiv 1 (\operatorname{mod} p)$ or $a + 1 \equiv 0 (\operatorname{mod} p) \Rightarrow a \equiv -1 (\operatorname{mod} p)$

So the set of integers $\{2, 3, ..., p - 2\}$ may be grouped into pairs a, a' such that $a \not\equiv a'$ and $aa' \equiv 1 (\operatorname{mod} p)$, Hence it follows that

$$2 \cdot 3 \cdot ... \cdot (p - 2) \equiv 1 (\operatorname{mod} p) \Rightarrow 2 \cdot 3 \cdot ... \cdot (p - 2)(p - 1) \equiv p - 1 (\operatorname{mod} p) \equiv -1 (\operatorname{mod} p)$$

i.e. $(p - 1)! \equiv -1 (\operatorname{mod} p)$

□

0.8.9. Example

Let $p = 13$ and consider the integers $2, 3, ..., 11$.

We have
$$\begin{aligned} 2 \cdot 7 &\equiv 1 (\operatorname{mod} 13) \\ 3 \cdot 9 &\equiv 1 (\operatorname{mod} 13) \\ 4 \cdot 10 &\equiv 1 (\operatorname{mod} 13) \\ 5 \cdot 8 &\equiv 1 (\operatorname{mod} 13) \\ 6 \cdot 11 &\equiv 1 (\operatorname{mod} 13) \end{aligned}$$

So $11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 (\operatorname{mod} 13)$.
Therefore $12! \equiv 12 \equiv -1 (\operatorname{mod} 13)$

The converse of Wilson's theorem is also true:

0.8.10. *Theorem:* converse of Wilson's theorem

> Suppose that $(n-1)! \equiv -1 (\operatorname{mod} n)$. Then n is prime.

Proof

Suppose that n is not prime and let d be a divisor of n with $1 < d < n$. Then $d \mid (n-1)!$. Since $n \mid \{(n-1)! + 1\}$ by hopothesis, it follows that $d \mid \{(n-1)! + 1\}$ also. This in turn implies that $d \mid 1$, which is a contradiction.

Although, this is completely useless as a primarlity test

$\square$

0.8.11. *Theorem*

> Suppose that p is an odd prime. Then the quadratic congruence $x^2 + 1 \equiv 0 (\operatorname{mod} p)$ has a solution if and only if $p \equiv 1 (\operatorname{mod} 4)$

Proof

Suppose that a is a solution of $x^2 + 1 \equiv 0(\operatorname{mod} p)$, so $a^2 \equiv -1(\operatorname{mod} p)$ Since $p \nmid a$ then Fermat's little theorem implies $1 \equiv a^{p-1}(\operatorname{mod} p) \equiv \left(a^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}(\operatorname{mod} p)(\dagger)$

Now suppose that $p = 4k + 3$ for some k. Then $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$ and so $(\dagger)$ implies that $-1 \equiv 1(\operatorname{mod} p)$. This implies that $p \mid 2$, which is a contradiction. Hence it follows that p must be of the form $4k + 1$

Conversely, suppose that $p = 4k + 1$ for some k.
Then $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-2) \cdot (p-1)(*)$

As a side note, note that we have the congruences $p - 1 \equiv -1(\operatorname{mod} p), p - 2 \equiv -2(\operatorname{mod} p), \ldots, \frac{p+1}{2} \equiv -\frac{p-1}{2}(\operatorname{mod} p)$

Rearranging the factors of $(*)$ gives $(p-1)! \equiv 1(-1) \cdot 2(-2) \cdot \ldots \cdot \frac{p-1}{2} \frac{-(p-1)}{2} \equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \ldots \cdot \frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2$ and by wilson's theorem we obtain $-1 \equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (1) \left[\left(\frac{p-1}{2}\right)!\right]^2$ and therefore we know that $\left[\left(\frac{p-1}{2}\right)!\right]^2$ is a solution to the congruence.

□

0.9. Jan 30 (Sara Ramirez's notes)

Arithmetical functions

0.9.1. *Proposition*

> Suppose p is prime. Then $\phi(p^q) = p^{q-1}(p-1)$

Proof

Consider the set of numbers $\{0, 1, 2, \ldots, p^q - 1\}$ The only numbers in this set that are not coprime to p are those that are divisible by p i.e. those of the form pt for $t = 0, 1, 2, \ldots, p^{q-1} - 1$. Therefore $\phi(p^q) = p^q - p^{q-1} = p^{q-1}(p-1)$

□

0.9.2. Definition: multiplicative function

Let $n = p_1^a \ldots p_r^{q_r}$
Suppose that $f : \mathbb{Z}^+ \to \mathbb{Z}$ is a function. f is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$
Examples: $f(n) = 1$ and $f(n) = n$ are multiplicative.

0.9.3. ***Proposition***

> If f is a multiplicative function and F is defined by $F(n) = \sum_{d|n} f(d)$ is also multiplicative.

Proof

Suppose that $m, n \in \mathbb{Z}^+$ such that $(m, n) = 1$

Then

$$F(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) \text{ since } (m, n) = 1$$

Recall that f is multiplicative, therefore we have $F(mn) = \sum_{d_1|m, d_2|n} f(d_1) f(d_2) =$ $(\sum_{d_1|m} f(d_1) \left(\sum_{d_2|n} f(d_2) \right) = F(m)F(n)$

□

0.9.4. ***Corollary:*** $d(n), \sigma(n)$ **are multiplicative**

> Recall that $d(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$

Proof

Then use the earlier examples of multiplicative functions and the above proposition.

□

0.9.5. *Theorem:* ϕ is multiplicative (proof 1)

> We can show thatthe euler function ϕ is multiplicative

Proof

Suppose that $m, n \in \mathbb{Z}$ such that $m, n > 1$ and $(m, n) = 1$, then consider the following array of integers:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & ... & m-1 \\ m & m+1 & m+2 & m+3 & ... & m+(m-1) \\ \vdots \\ (n-1)m & (n-1)(m)+1 & ... & ... & ... & (n-1)m+(m-1) \end{pmatrix}$$

The (cool thing) is that this array consists of mn consecutive integers, and so it is a complete set of residues mod mn. If follows that $\phi(mn)$entries of this array are coprime to mn. The first row is a complete set of residues mod m and all the entries in any given column are congruent mod m. Therefore there are exactly $\phi(m)$ columns consisting of integers that are coprime to m.

Consider such a column, It's entries are of the form $\alpha, m + \alpha, 2m + \alpha + ... + (n - 1)m\alpha$ for some α.There are n integers, no 2 of which are congruent mod n. Therefore there are $\phi(n)$ integers in each column that are coprime to n

Hence there are $\phi(m)\phi(n)$ leements in the array that are coprime to both m and n, and hence mn. Which shows that ϕ is multiplicative since i.e. $\phi(mn) = \phi(m)\phi(n)$

□

0.9.6. *Corollary*

> $$\left(\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)\right)$$

Proof

Let n have prime factorization $n = p_1^{q_1} ... p_k^{q_k}$

Then $\phi(n) = \phi(p_1^{q_1} ... p_k^{q_k}) = \phi(p_1^{q_1}) ... \phi(p_k^{q_k}) = p_1^{q_1 - 1}(p_1 - 1) ... p_k^{q_k - 1}(p_k - 1) = p_1^{q_1}\left(1 - \frac{1}{p_1}\right) ... p_k^{q_k}\left(1 - \frac{1}{p_k}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Note that in the third equality we use 0.9.1

□

0.10. Feb 4

0.10.1. ***Theorem:*** **ϕ is multiplicative (proof 2)**

Proof

0.10.2. ***Corollary***

If n is a positive integer then $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Proof

See the earlier proof

□

2nd proof that ϕ is multiplicative.

Let $p_1 \ldots, p_k$ be distinct prime factors of n. Then

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right) = n - \sum\left(\frac{n}{p_1}\right) + \sum\left(\frac{n}{p_1 p_2}\right) - \sum \frac{n}{p_1 p_2 p_3} + \ldots$$

motivation: suppose that $n = p_1 p_2$ then $n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right) = n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2}$ (take away integers that are divisible by p_1, p_2 and add back in integers $1 \ldots n$ that are divisible by $p_1 \wedge p_2$)

Now: $n = \sum_{m=1}^{n} 1$ and note that $\frac{n}{p_r}$ denotes the number of integers in the set $\{1, 2, \ldots, n\}$ that are divisible by p_r therefore

$$\sum_{1 \leq r \leq k} \frac{n}{p_r} = \sum_{m=1}^{n} \sum_{1 \leq r \leq k, P_r | m} 1$$

For each integer m with $1 \leq m \leq n$ let $l(m) :=$ the no. of primes in $\{p_1, \ldots p_k\}$ that divide m.

Then we have

$$n - \sum_{1 \leq r \leq k} \frac{n}{p_r} + \sum_{1 \leq s < r \leq k} \frac{n}{p_r p_s} - \sum_{1 \leq t < s < r \leq k} \frac{1}{p_r p_s p_t} + \ldots =$$

$$\sum_{m=1}^{n} \left(1 - \sum_{r, P_r | m} 1 + \sum_{r > s, P_r, P_s | m} 1 - \ldots\right) = \sum_{m=1}^{n} \left(1 - \binom{l(m)}{1} + \binom{l(m)}{1} - \binom{l(m)}{3} + \ldots\right)$$

Let $\left(1 - \binom{l(m)}{1} + \binom{l(m)}{1} - \binom{l(m)}{3} + \ldots\right)(\star)$

Then if $l(m) = 0$ them $(\star)$ is equal to 1, i.e. if $(m, n) = 1$ then $(\star)$ is 1.

Also, if $l(m) > 0$ them $(\star)$ is equal to $(1 - 1)^{l(m)} = 0$.

Then we have $\sum_{m=1}^{n} \left[\left(1 - \binom{l(m)}{1} + \binom{l(m)}{2} - \binom{l(m)}{3} + \ldots\right)\right] = \sum_{m,(m,n)=1} 1 = \phi(n)$

□

□

0.10.3. ***Theorem***

> Suppose that $n > 0$ then $\sum_{d|n} \phi(d) = n$

Proof

Proof 1: Let $S = \{1, 2, ..., n\}$. For each $d \mid n$ le $C_d = \{a \in S : (a, n) = d\}$ Then $S = \cup_{d|n} C_d$ and $C_d \cap C_{d'} = \emptyset$ if $d \neq d'$,

Now suppose that $a \in C_d$. Then we may write $a = bd$ where $1 \leq b \leq \frac{n}{d}$ and $\left(b, \frac{n}{d}\right) = 1$.

So, $|C_d| = |\{a \in S : (a, n) = d\}| = |\left\{1 \leq b \leq \frac{n}{d} : \left(b, \frac{n}{d}\right) = 1\right\} = \phi\left(\frac{n}{d}\right)$

Hence $n = \sum_{d|n} |C_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$

Proof 2: Define a function F by $F(n) = \sum_{d|n} \phi(d)$. Then, since ϕ is multiplicative, we have that F is multiplicative.

Now suppose that $n = p^j$ where p is prime. Then $F(p^j) = \sum_{d|p^j} \phi(d) = \sum_{i=0}^{j} \phi(p^i) = 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + ... + (p^j - p^{j-1}) = p_j$

$\square$

0.10.4. Definition: μ mobius function

The Mobius function $\mu : \mathbb{Z}^+ \to Z$ is defined by

1 if $n = 1$
0 if $p^2 \mid n$ for some prime p
$(-1)^r$ if $n = p_1 p_2 ... p_r$ where the p_i are distinct primes.

For example $\mu(2) = 1, \mu(6) = 1, \mu(4) = 0$

0.10.5. ***Theorem***

> The function μ is multiplicative

Proof

Suppose that $m, n \in \mathbb{Z}^+$ with $(m, n) = 1$. If either $p^2 \mid m$ or $p^2 \mid n$ for some p, them $p^2 \mid mn$ and so we have $\mu(mn) = 0 = \mu(m) \cdot \mu(n)$

Suppose therefore that m, n are such that $m = p_1 \cdot p_r, n = q_1 ... q_s$ where $\left(p_i, q_j\right)$ are distinct primes. Then $\mu(mn) = \mu(p_1 ... p_r q_1 ... q_s) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m) \cdot \mu(n)$

$\square$

0.10.6. ***Theorem***

> For each positive integer $n \geq 1$, we have $\sum_{d|n} \mu(d) = 1$ if n=1, 0 if n > 1

Proof

First observe that $\sum_{d|1} \mu(d) = \mu(1) = 1$.

Now consider the function F defined by $F(n) = \sum_{d|n} \mu(d)$. Since μ is multiplicative, we have that F is multiplicative also. Suupose that p is a prime and $k \geq 1$. Then

$$F(p^k) = \sum_{d|p^k} \mu(p^k) = \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^k) = \mu(1) + \mu(p) = 1 - 1 = 0$$

So if $n > 1$ with $n = p_1^{k_1} ... p_r^{k_r}$ then $F(n) = F(p_1^{k_1}) ... F(P_r^{k_r})) = 0$

□

0.10.7. ***Theorem:*** **Mobius Inversion Formula**

> Suppose that f and F are two (not necessarily multiplicative!) functions $f, F : \mathbb{Z}^+ \to \mathbb{Z}$ related by the function $F(n) = \sum_{d|r} f(d)$. Then $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$

Proof

Proof: compute

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} (\mu(d) \sum_{c|\left(\frac{n}{d}\right)} f(c) = \sum_{d|n} \left(\sum_{c|\left(\frac{n}{d}\right)} \mu(d) f(c) \right) (\dagger)$$

Now observe that $d \mid n$ and $c \mid \frac{n}{d}$ if and only if $c \mid n$ and $d \mid \frac{n}{c}$. To see this: $d \mid n \Rightarrow n = ad, c \mid \frac{n}{d} \Rightarrow \alpha = cp$ and so we have $n = \alpha d = cpd \Rightarrow c \mid d$ and $d \mid \frac{n}{c}$

Now $\sum_{d|\frac{n}{c}} \mu(d) = 0$ if $n \neq c, 1$ if $n = c (\star)$

Hence

$$\sum_{d|m} \left(\sum_{c|\frac{n}{d}} \mu(d) f(c) \right) = \sum_{d|n} \left(\sum_{d|\frac{n}{c}} f(c) \mu(d) \right) = \sum_{c|n} \left(f(c) \sum_{d|\frac{n}{c}} \mu(d) \right) (\dagger)$$

Now apply $\star$ to the RHS of $(\dagger)$ to obtain: $\sum_{c|n} (f(c) \sum_{d|\frac{n}{c}} \mu(d) = \sum_{c|n} f(c) \sum_{d|\frac{n}{c}} \mu(d) = f(n)$ as required.

□