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 $m \nmid n$

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.

□

0.3.2. *Theorem*

> There are infinitely many positive primes

Proof:

Suppose that there are only finitely many positive primes.

Consider the integer $N = p_1 \ldots p_2 \ldots p_r + 1$. 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 $p_1, \ldots, p_r$ such that p divides N. (this leads to a contradiction)

□

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

$$0 < m^2 < m < 1 \Rightarrow$$
$$0 < m^3 < m^2 < m < 1 \Rightarrow$$
$$0 < m^4 < m^3 < \ldots$$

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

□

0.3.4. ***Theorem***

> The real number e is irrational

Proof:

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

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

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

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

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 $r_n < \frac{b}{n+1} + b\left(\frac{1}{(n+1)(n+2)} + \frac{1}{(n+2)(n+3)} + \ldots\right) = \frac{b}{n+1} + b\left(\left(\frac{1}{n+1} - \frac{1}{n+2}\right) + \left(\frac{1}{n+2} - \frac{1}{n+3}\right) + \ldots\right) = \frac{b}{n+1} + \frac{b}{n+1} = 2\frac{b}{n+1}$

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)

□

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

□

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.

□

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 ...

□

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 $2^2\cdot 3^2=36$

□

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

□

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)

□

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 $ax + by = n$ $(\dagger)$

Remarks:

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

First, solve $ax_1 + by_1 = h$

Then set $x = mx_1, y = my_1$

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

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

4. Now suppose that $h > 1$, and $n = mh$ so $(\dagger)$ 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 $(\dagger)$

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 $(\dagger)$ 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 $a \equiv b (\mathrm{mod}\, m)$ or $a \equiv b(m)$
(Informally, "equality except for the addition of some multiple of m")

Examples: $63 \equiv 0 \bmod 3, 7 \equiv -1 \bmod 8, 5^2 \equiv -1 \bmod 13$

Additionally, note that $x \equiv y \bmod 2 \Leftrightarrow$ x and y are both even or x and y are both odd

0.6.5. Remark

If $a \equiv \alpha, b \equiv \beta \bmod m$ then

$$a + b \equiv \alpha + \beta \bmod m,$$
$$a - b \equiv \alpha - \beta \bmod m,$$
$$ab \equiv \alpha\beta \bmod m$$

Proof:

Since $a \equiv \alpha \bmod m$ and $b \equiv \beta \bmod m$ 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 $a + b \equiv \alpha + \beta \bmod m$ □

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 $42 \equiv 12 \bmod 10$ however $\frac{42}{6} \not\equiv \frac{12}{6} \bmod 10$

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

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

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 $\{0, 1, 2, ..., m-1\}$. 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 $ax \equiv b (\mathrm{mod}\, m)$ $(\dagger)$

0.7.2. *Theorem*

> The congruence $(\dagger)$ 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 $(\dagger)$ 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 $\dagger$ it suffices to solve $a'x \equiv b' (\mathrm{mod}\, m') (\dagger\dagger)$

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

Hence $(\dagger\dagger)$ has precisely one solution modulo m'

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

□

0.7.3. Example

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

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

0.7.5. *Corollary*

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

0.7.6. Remark

The congruence $ax \equiv b (\mathrm{mod}\, m)$ 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 $x \equiv c_j \pmod{n_j}, 1 \leq j \leq k$ (†)

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 $m_j x_j \equiv c_j \pmod{n_j}$ (†)
The integer $x = m_1 x_1 + ... + m_k x_k$ satisfies $x \equiv c_j \pmod{n_j}$

□

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 $x \equiv 0 + m_2 x_2 + 0 + 0 + ... + 0 (\mathrm{mod}\, n_2) \equiv c_2 (\mathrm{mod}\, n_2)$

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 $x \equiv y \pmod{n_j}$ i.e. $x - y \equiv 0 \pmod{n_j}$.

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

0.7.10. Example

Consider $x \equiv 2(\text{mod } 5), x \equiv 3(\text{mod } 7), x \equiv 4(\text{mod } 11)$.

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: $77x_1 \equiv 2(\text{mod } 5), 55x_2 \equiv 3(\text{mod } 7), 35x_3 \equiv 4(\text{mod } 11)$

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

A solution is given by $x = 77x_1 + 55x_2 + 35x_3$ 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 $x(\text{mod } m)$ is the smallest positive integer l satisfying $x^l \equiv 1(\text{mod } m)$

0.7.12. Example

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

0.7.13. *Proposition*

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

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 $x^k \equiv x^h(\text{mod } m)$.

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

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 $x \,\text{mod}\, m$ is the smallest positive integer l satisfying $x^l \equiv 1(\text{mod } m)$

0.8.2. *Proposition*

We have that $x^n \equiv 1(\text{mod } m)$ 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. $\binom{p}{r} \equiv 0 (\mathrm{mod}\, p)$

Now suppose that x, y are intleterninates. Then

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

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

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

0.8.4. *Theorem:* Fermat's Little Theorem

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

Proof:

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

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

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

□

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

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

In other words $x\alpha_1 \ldots x\alpha_{\phi(m)} \equiv \alpha_1 \ldots \alpha_{\phi(m)} (\mathrm{mod}\, m)$

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

□

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 $3, 9, 1, 7, 13, 19, 11, 17 (\text{mod } 20)$.

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

0.8.8. *Theorem:* Wilson's Theofrem

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

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 $aa' \equiv 1 (\text{mod } p)$

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

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

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

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

□

0.8.9. Example

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

$2 \cdot 7 \equiv 1 (\text{mod } 13)$

$3 \cdot 9 \equiv 1 (\text{mod } 13)$

$4 \cdot 10 \equiv 1 (\text{mod } 13)$

$5 \cdot 8 \equiv 1 (\text{mod } 13)$

We have $6 \cdot 11 \equiv 1 (\text{mod } 13)$

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

The converse of Wilson's theorem is also true:

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

> Suppose that $(n-1)! \equiv -1 (\mathrm{mod}\, n)$. 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

□

0.8.11. ***Theorem***

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

Proof:

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

Now suppose that $p = 4k + 3$ for some k. Then $(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$ and so $(\dagger)$ implies that $-1 \equiv 1 (\mathrm{mod}\, p)$. 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 $p - 1 \equiv -1 (\mathrm{mod}\, p), p - 2 \equiv -2 (\mathrm{mod}\, p), \ldots, \frac{p+1}{2} \equiv -\frac{p-1}{2} (\mathrm{mod}\, p)$

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 $n = p_1^a ... p_r^{q_r}$
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:

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

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 $\alpha, m+\alpha, 2m+\alpha+\dots+(n-1)m\alpha$ 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*

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

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

$$n\prod_{p|n}\left(1-\frac{1}{p}\right) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right) = n - \sum\left(\frac{n}{p_1}\right) + \sum\left(\frac{n}{p_1p_2}\right) - \sum\frac{n}{p_1p_2p_3} + ...$$

motivation: suppose that $n = p_1p_2$ then $n\prod_{p|n}\left(1-\frac{1}{p}\right) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right) = n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1p_2}$ (take away integers that are divisible by p_1, p_2 and add back in integers $1...n$ 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 $\{1, 2, ..., n\}$ that are divisible by p_r therefore

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

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

Then we have

$$n - \sum_{1\le r\le k}\frac{n}{p_r} + \sum_{1\le s<r\le k}\frac{n}{p_rp_s} - \sum_{1\le t<s<r\le k}\frac{1}{p_rp_sp_t} + ... =$$

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

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

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

□

□

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 $F(p^j) = \sum_{d|p^j} \phi(d) = \sum_{i=0}^{j} \phi(p^i) = 1 + (p-1) + (p^2 - p) + (p^3 - p^2) + ... + (p^j - p^{j-1}) = p_j$

□

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 $\mu(mn) = \mu(p_1 ... p_r q_1 ... q_s) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \mu(m) \cdot \mu(n)$

□

0.10.6. ***Theorem***

> For each positive integer $n \geq 1$, we have $\sum_{d|n} \mu(d) = 1$ if n=1, $\sum_{d|n} \mu(d) = 0$ 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 $F(n) = F\left(p_1^{k_1}\right) ... F\left(P_r^{k_r}\right)) = 0$

□

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

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.

□

0.11. Feb 11

0.11.1. *Theorem:* Mobius Inversion Formula

Suppose that F and f are two arithmetic functions (not necessarily multiplicative!) such that $f, F : \mathbb{Z}^+ \to \mathbb{Z}$ Assume that f and F are related by the formula $F(n) = \sum_{d|n} f(d)$.

Then

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

0.11.2. Example:

Recall that $d(n) = \sum_{d|n} 1$ and $\sigma(n) = \sum_{d|n} d$.
Then by Mobius inversion, we have that $1 = \sum_{c|n} \mu\left(\frac{n}{c}\right) d(c)$ and $n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d)$ (?)

0.11.3. *Theorem*

Suppose that F is a multiplicative function, and that $F(n) = \sum_{d|n} f(d)$ for some f. Then, f is also multiplicative

Proof:

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

$$f(mn) = \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) = \sum_{d_1|m, d_2|n} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) = \sum_{d_1|m, d_2|n} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) =$$

$$\sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|m} \mu(d_2) F\left(\frac{n}{d_2}\right) = f(m) f(n)$$

□

0.11.4. *Corollary*

The function ϕ is multiplicative

Proof:

Earlier we used a counting argument to show that $n = \sum_{d|n} \phi(d)$

This argument did not appeal to the fact that ϕ is multiplicative!

Since $F(n) = n$ is clearly multiplicative, it follows that ϕ is multiplicative.

□

0.11.5. ***Theorem***

> For any positive integer n, we have $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$

Proof:

Apply the Mobius inversion formula to $F(n) = n = \sum_{d|n} \phi(d)$

The result if $\phi(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \frac{n}{d}$

□

0.11.6. Remark

We can determine the value of $\phi(n)$. Suppose that $n = p_1^{q_1} ... p_k^{q_k}$. Then applying the last theorem gives us

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{i=1}^{k} \left(\mu(1) + \frac{\mu(p_2)}{p_2} + \frac{\mu(p_i^2)}{p_i^2} + ... + \frac{\mu\left(p_i^{q_i}\right)}{p_i^{q_i}} \right)$$

Hence $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

0.11.7. Primitive Roots and Indices

0.11.8. Note

Recall: suppose that $n > 1$ and that $(a, n) = 1$. Then the order of $a (\mathrm{mod}\, n)$ is the smallest positive integer k such that $a^k \equiv 1 (\mathrm{mod}\, n)$

0.11.9. ***Theorem***

> Suppose that a has order $k (\mathrm{mod}\, n)$. Then $a^h \equiv 1$ if and only if $k \mid h$. In particular $k \mid \phi(n)$

Proof:

For any $h \in \mathbb{Z}^+$ we may write $h = qk + r$ where $0 \leq r < k$

Then $a^h \equiv 1 (\mathrm{mod}\, n)$ if and only if $a^{qk+r} \equiv 1 (\mathrm{mod}\, n)$ if and only if $a^r \equiv 1 (\mathrm{mod}\, n)$ if and only if $r = 0$

□

0.11.10. ***Corollary***

> Suppose that a has order $k \pmod n$. Then $a^i \equiv a^j (\mathrm{mod}\, n)$ if and only if $i \equiv j (\mathrm{mod}\, k)$

Proof:

Suppose that $i \geq j$ then $a^i \equiv a^j (\mathrm{mod}\, n)$ if and only if $a^{i-j} \equiv 1 (\mathrm{mod}\, n)$ if and only if $k \mid (i - j)$ if and only if $i \equiv j (\mathrm{mod}\, k)$

□

0.11.11. ***Corollary***

> If a has order $k (\mod n)$ then the integers $a, a^2, a^3, ...a^k$ are pairwise incongruent modulo n

Proof:

□

0.11.12. ***Theorem***

> Suppose that a has order $k (\mod n)$, and that $h > 0$. Then we claim that a^h has order
>
> $$\frac{k}{(h,k)} (\mod n)$$

Proof:

Set $d = (h, k)$. Then we may write $h = h_1 d, k = k_1 d$ with $(h_1, k_1) = 1$

Note that $\left(a^h\right)^{k_1} = \left(a^{h_1 d}\right)^{\frac{k}{d}} = \left(a^k\right)^{h_1} \equiv 1 (\mod n)$. So if r is the order of $a^h (\mod n)$, then $r \mid k_1 (\star)$

On the other hand, $a^{hr} = \left(a^h\right)^r \equiv 1 (\mod n)$ and so $k \mid hr$ i.e. $k_1 d \mid h_1 dr$ i.e. $k_1 \mid h_1 r$. Since $(h_1, k_1) = 1$ this implies that $k_1 \mid r$, so $k = k_1 d = rd$. Then it follows from $(\star)$ that $r = \frac{k}{d} = \frac{k}{(h,k)}$, as claimed.

□

0.11.13. ***Corollary***

> Suppose that a has order $k \bmod(n)$. Then a^h has order $k (\mod n)$ if any only if $(h, k) = 1$

0.11.14. Example: Of the above

We can first make a table that integers $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ have order $1, 12, 3, 6, 4, 12, 12, 4, 3, 6, 12, 2$

By the previous theorem,

The order of $2 (\mod 13)$ is 12

The order of $2^2 (\mod 13)$ is $\frac{12}{(2,12)} = \frac{12}{2} = 6$

The order of $2^3 (\mod 13)$ is $\frac{12}{(3,12)} = \frac{12}{3} = 4$

The integers having order 12 (mod 13) are powers of 2^k for which $(k, 12) = 1$ i.e. $2^1 \equiv 2, 2^2 \equiv 6, 2^3 \equiv 11, 2^{11} \equiv 7 (\mod 13)$ (here the congruences denote a mapping to the order)

0.11.15. Definition

If $(a, n) = 1$ and a has order $\phi(n) (\mod n)$ then we say that a is a primitive root $(\mod n)$

i.e. a is a primitive root $(\mod n)$ if $a^{\phi(n)} \equiv 1 (\mod n)$ but $a^k \not\equiv 1 (\mod n) \forall 1 \leq k < \phi(n)$

For example 2 is a primitive root $(\mod 13)$

0.11.16. ***Proposition***

> Suppose that $n > 1$ such that $p = 2^{2^n} + 1$ is prime. Then 2 is not a primitive root $(\mathrm{mod}\, p)$

Proof:

Since $2^{2^{2n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = p(2^{2^n} - 1)$

We have that $2^{2^{n+1}} \equiv 1 (\mathrm{mod}\, p)$. So the order of 2 $(\mathrm{mod}\, p)$ is at most 2^{n+1}

On the other hand, since p is prime, we have $\phi(p) = p - 1 = 2^{2^n}$ Now since $2^{2^n} > 2^{n+1}$ (prove this!), it follows that 2 is not a primitive root $(\mathrm{mod}\, p)$

□

0.11.17. ***Theorem***

> Suppose that $(a, n) = 1$ and let $\alpha_1, \alpha_2, ..., \alpha_{\phi(n)}$ be the set of positive integers less than n and coprime to n. If a is a primitive root $(\mathrm{mod}\, n)$ then the set $a, a^2, ..., a^{\phi(n)}$ is congruent mod n to $\alpha_1, ..., \alpha_{\phi(n)}$ in some order.

0.11.18. ***Corollary***

> Suppose that a primitive root $(\mathrm{mod}\, n)$ exists. Then there are exactly $\phi(\phi(n))$ primitive roots $(\mathrm{mod}\, n)$

Proof: Suppose that a is a primitive root $(\mathrm{mod}\, n)$ Then any other primitive root lies in the set $\{a, a^2, ..., a^{\phi(n)}\}$ The number of powers $a^k (1 \leq k \leq \phi(n))$ that have order $\phi(n)$ =the number of integers $k (1 \leq k \leq \phi(n))$ for which $(k, \phi(n)) = 1 = \phi(\phi(n))$

□

0.12. Feb 13

Primitive roots moudlo primes

0.12.1. ***Theorem***

> We can show that there exists a primitive root modulo every prime p

0.12.2. *Theorem:* Lagrange

> Suppose that p is a prime and that $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ where $a_i \in \mathbb{Z}, a_n \not\equiv 0 (\mathrm{mod}\, p)$
>
> Then the congruence $f(x) \equiv 0 (\mathrm{mod}\, p) (\dagger)$ has at most n distinct solutions modulo p

Proof:

This is related to the fact that a polynmial of degree n has at most n solutions. This theorem is a "modulo" version of that

The proof is by induction on the degree n of $f(x)$

Suppose that $n = 1$ Then $f(x) = a_1 x + a_0$. Since $(a_1, p) = 1$ the congruence $f(x) \equiv 0 (\mathrm{mod}\, p)$ has a unique solution $\mathrm{mod}\, p$

Now suppose that degree of $f(x) = k$, and that the result holds for all polynomials of degree at most $k - 1$

If $(\dagger)$ has no solutions, then we are done.

Next, suppose that $x \equiv a (\mathrm{mod}\, p)$ is a solution of $(\dagger)$

Then $f(x) = (x - a)q(x) + r$, with the degree of $q(x) = k - 1$

We have $f(a) \equiv 0 (\mathrm{mod}\, p)$ and this implies that $r \equiv 0 (\mathrm{mod}\, p)$ Hence $f(x) \equiv (x - a)q(x) (\mathrm{mod}\, p)$

Now if $x \equiv b (\mathrm{mod}\, p)$ is a solution of $(\dagger)$, with $b \not\equiv a (\mathrm{mod}\, p)$, then we have $f(b) \equiv 0 (\mathrm{mod}\, p) \Rightarrow (b - a)q(b) \equiv 0 (\mathrm{mod}\, p) \Rightarrow q(b) \equiv 0 (\mathrm{mod}\, p)$

So any solution of $(\dagger)$that is different from a must satisfy $q(x) \equiv 0 (\mathrm{mod}\, p) (\star)$

Since, by our inductive hypothesis, $(\dagger)$ has at most $k - 1$ distinct solutions $(\mathrm{mod}\, p)$, then it follows that $(\dagger)$ has at most k distinct solutions $\mathrm{mod}\, p$

This completes the induction step, and so the theorem follows by induction

□

0.12.3. *Corollary*

> Suppose that p is a prime and that $d \mid (p - 1)$, then the congruence $x^d - 1 \equiv 0 (\mathrm{mod}\, p)$ has exactly d solutions.

Proof:

Since $d \mid (p - 1)$, we have $p - 1 = dk$ for some k

Therefore $x^{p-1} - 1 = \left(x^d - 1\right) f(x)$ where $f(x) = x^{d(k-1)} + x^{d(k-2)} + ... + x^d + 1$
and degree of $f(x) = d(k - 1) = p - 1 - d$

Therefore Langrange's theorem implies that $f(x)$ has at most $p - 1 - d$ distinct solutions $(\mathrm{mod}\, p)$

Euler's theorem implies that $x^{p-1} - 1$ has exactly $p - 1$ distinct roots $(\mathrm{mod}\, p)$

Hence $x^d - 1$ has at least $(p - 1) - (p - 1 - d) = d$ distinct roots $(\mathrm{mod}\, p)$

□

0.12.4. *Theorem:* Alternative proof of wilson's theorem

> Recall that Wilson's theorem says that $(p-1)! \equiv -1 (\mod p)$ is p is prime.

Proof:

Define a polynomial $f(x) = (x-1)(x-2)...(x-(p-1)) - (x^{p-1}-1) = \alpha_{p-2}x^{p-2} + \alpha_{p-3}x^{p-3} + ... + \alpha_1 x + \alpha_0$ with degree $p-2$

Fermat's little theorem implies that the congruence $f(x) \equiv 0 (\mod p)$ has solutions $1, 2, 3, ..., p-1 \ (\mod p)$, these are all distinct solutions and therefore contradict Langrange's theorem (unless $\alpha_{p-2} = \alpha_{p-3} = ... = \alpha_0 (\mod p)$ i.e. $f(x) = 0$)

Therefore for all integers x we have $f(x) \equiv 0 (\mod p)$ and taking $x = 0$ gives $(-1)(-2)...(-(p-1)) + 1 \equiv 0 (\mod p)$ i.e. $(-1)^{p-1}(p-1)! \equiv -1 (\mod p)$ i.e. $(p-1)! \equiv -1 (\mod p)$

□

0.12.5. ***Theorem***

> Suppose that p is a prime and that $d \mid (p-1)$
>
> Then there exist exactly $\phi(d)$ distinct integers $\bmod p$ that have order $d \bmod p$

Proof:

We have shown that the congruence $x^d \equiv 1 (\bmod p)$ has exactly d solutions.

For each $c \mid d$ let $\psi(c)$ =the number of integers in the set $1, 2, ..., p-1$ that have order c

Then $d = \sum_{c|d} \psi(c)$

Applying Mobius inversion gives $\psi(d) = \sum_{c|d} \mu(c) \cdot \frac{d}{c} = \phi(d)$

0.12.6. Example

Let $p = 13$ then 1 has order 1, 12 has order 2, 3 and 9 have order 3, 5 and 8 have order 4, 4 and 10 have order 6, and 2,6,7,11 have order 12

Then we can easily check that (i) $\sum_{d|12} \psi(d) = 12$ and that (ii) $\psi(d) = \phi(d) \forall d \mid 12$

0.12.7. ***Corollary***

> If p is a prime, then there are exactly $\phi(p-1)$ primitive roots $\bmod p$

0.12.8. Example

If p is a prime of the form $4k+1$ then $x^2 \equiv -1 (\bmod p)$ has a solution

Proof: We have that $4 \mid (p-1)$, so there exists an integer a such that a has order $4 \bmod p$ Then $a^4 \equiv 1 (\bmod p)$ if and only if $(a^2-1)(a^2+1) \equiv 0 (\bmod p)$

Now if $a^2 - 1 \equiv 0 (\bmod p)$ then a has order $2 \bmod p$ which is a contradiction. So $a^2 + 1 \equiv 0 (\bmod p)$ i.e. $a^2 \equiv -1 (\bmod p)$

□

some additional remarks ...

0.12.9. Remark

Why does the decimal expansion of $\frac{1}{7} = 0.14285714...$ have period 6, while $\frac{1}{11} = 0.0909...$ have period 2?

Suppose that p is a prime, and that 10 has order $k \bmod p$ i.e. $10^k \equiv 1 (\bmod p)$ and k is the smallest positive integer for which this holds. Then $10^k - 1 = Np$ for some $N \in \mathbb{Z}_{\geq 0}$

Therefore

$$\frac{1}{p} = \frac{N}{10^k - 1} = \frac{N}{10^k} \cdot \frac{1}{1 - \frac{1}{10^k}} = \frac{N}{10^k}\left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + ...\right)$$

Since $\frac{1}{p} < 1$ we must have $\frac{N}{10^k} < 1$ i.e. $\frac{N}{10^k} = 0.\alpha_1\alpha_2...\alpha_k$ say.

So $\frac{1}{p} = (0.\alpha_1\alpha_2...\alpha_k)(1 + \frac{1}{10^k} + \frac{1}{10^{2k}}... + ...)$

We therefore see that the decimal expansion of $\frac{1}{p}$ has period k

Consequence: Since Euler's theorem implies that $10^{p-1} \equiv 1 (\bmod p)$ we have $1 \leq k \leq p - 1$

The decimal expansion of $\frac{1}{p}$ has period $p - 1$ if and only if 10 is a primitive root mod p

Conjecture: This happens for infinitely many primes.

0.12.10. Problem 1

> Given any non-zero integer a other than $1, -1$, or a perfect square, there exist infinitely many primes p such that a is a primitive root mod p

Solution

This is an open problem

0.12.11. *Theorem*

> One of 2,3,5 is a primitive root mod p for inifintely many primes p

Proof: See Murty "Artin's conjecture for primitive roots" in mathematical intelligences vol 10 no 4 (Fall 1988)

□

0.13. Feb 18

0.13.1. Example

2 is a primitive root mod 9

For which composite numbers n do there exist primitive roots mod n ?

0.13.2. ***Lemma***

If a is an odd integer and $k \geq 3$, then

$$a^{2^{k-1}} \equiv 1 \pmod{2^k} (\dagger)$$

Proof:

The proof is by induction on k

If $k = 3$ the congruence is $a^2 \equiv 1 \pmod 8$

Suppose that $(\dagger)$ holds for some $k \geq 3$ then

Then for some $b \in \mathbb{Z}_{>0}$ we have

$$a^{2^{k-2}} = 1 + b \cdot 2^k$$

Hence

$$\left(a^{2^{k-2}}\right)^2 = \left(1 + b \cdot 2^k\right)^2 \Rightarrow a^{2^{k-1}} = 1 + 2^{k+1}\left(b + b^2 \cdot 2^{k-1}\right) \equiv 1 \pmod{2^{k+1}}$$

Hence if $(\dagger)$ holds for some $k \geq 3$, then it also holds for $k + 1$, and the result now follows by induction

□

0.13.3. ***Theorem***

If $k \geq 3$ then there are no primitive roots mod 2^k

Proof:

The integers corpime to 2^k are precisely the odd integers. Furthermore $\phi\left(2^k\right) = 2^{k-1}$

If a is odd, then the lemma implies that $a^{\phi(2^k)/2} = a^{(2^k-1)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}$

Therefore there are no primitive roots mod 2^k

□

0.13.4. ***Theorem***

> If $m > 2$ and $n > 2$ with $(m, n) = 1$, then there are no primitive roots mod mn

Proof:

Suppose that $a \in \mathbb{Z}_{>0}$ with $(a, mn) = 1$

Then $(a, m) = 1$ and $(a, n) = 1$ since $(m, n) = 1$

Also $\phi(m)$ and $\phi(n)$ are even.

$$\therefore a^{\frac{1}{2}\phi(mn)} = \left(a^{\phi(m)}\right)^{\frac{1}{2}\phi(n)} \equiv 1 (\mathrm{mod}\, m)$$

Also

$$a^{\frac{1}{2}\phi(mn)} = \left(a^{\phi(m)}\right)^{\frac{1}{2}\phi(n)} \equiv 1 (\mathrm{mod}\, n)$$

Since $(m, n) = 1$, this implies that $a^{\frac{1}{2}\phi(mn)} \equiv 1 (\mathrm{mod}\, mn)$

So there are no primitive roots mod mn

□

0.13.5. ***Corollary***

> There are no primitive roots mod n if either
> (i) n is divisible by two odd primes, or
> (ii) n is of the form $2^m \cdot p^k$ where p is an odd prime, and $m \geq 2$

Proof:

Hence the only possibilities for which a primitive root mod n can exist are $n = 2, 4, p^k, 2p^k$ where p is an odd prime.

□

0.13.6. ***Lemma***

> If p is an odd prime, then there exists a primitive root $r \pmod p$ such that
>
> $$r^{p-1} \not\equiv 1 \pmod{p^2}$$

Proof:

Let r be any primitive root mod p (we have shown that such an r exists)

If $r^{p-1} \not\equiv 1 (p^2)$ then we are done

Otherwise, consider $r_1 := r + p$. Then r_1 is a primitive root mod p, and

$$r_1^{p-1} = (r+p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \bmod (p^2) \not\equiv 1 \pmod{p^2}$$

since $p \nmid r^{p-2}$

□

0.13.7. ***Corollary***

> IF p is an odd prime, then p^2 has a primitive root.

Proof:

Let r be a primitive root mod p

Then the order of $r \bmod (p^2)$ is either $p-1$ or $\phi(p^2) = p(p-1)$

(The order cannot be p because $r^p \equiv r \pmod p$)

Then Lemma 0.13.6 implies that if r has order $p-1 \bmod p^2$, then $r+p$ is a primitive root $\bmod r^2$

□

0.13.8. ***Lemma***

> Let p be an odd prime and let r be a primitive root mod p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$ Then for each integer $k \geq 2$ we have
>
> $$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k} (\dagger)$$

Proof:

The proof is by induction on k

By hypothesis, $(\dagger)$ holds for $k = 2$

Let $k \geq 2$ be an integer for which $(\dagger)$ holds.

Since $(r, p) = 1$ we have $\left(r, p^{k-1}\right) = 1$

So Euler's theorem implies that

$$r^{(p-1)p^{k-2}} = r^{\phi(p^k - 1)} \equiv 1 \pmod{p^{k-1}}$$

$\therefore r^{(p-1)p^{k-2}} = 1 + ap^{k-1}$ (and $p + a$ by our inductive hypothesis)

$\therefore \left(r^{(p-1)p^{k-2}}\right)^2 = \left(1 + ap^{k-1}\right)^p \Rightarrow r^{(p-1)p^{k-2}} \equiv 1 + ap^k \pmod{p^{k+1}} \Rightarrow r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^{k+1}}$ since $p \nmid a$

Hence if $(\dagger)$ holds for k, then it holds for k_1

This completes the induction step and proves the lemma.

□

0.13.9. ***Theorem***

> If p is an odd prime and $k \geq 1$, then there exists a primitive root $\bmod p^k$

Proof:

Lemmas 0.13.6 and 0.13.8 imply that there exists a primitive root $r(\bmod p)$ such that

$$r^{p^{k-2}(p-1)} \not\equiv 1\left(\bmod p^k\right)(\star)$$

Claim: r is a primitive root $\bmod p^k$

Let n be the order of $r\left(\bmod p^k\right)$

Then $n \mid \phi\left(p^k\right)$ i.e. $n \mid p^{k-1}(p-1)$

Now $r^n \equiv 1\left(\bmod p^k\right)$ and so $r^n \equiv 1(\bmod p)$

The order of $r(\bmod p)$ is $p-1$ and so $(p-1) \mid n$

$\therefore$ we have $n = p^m(p-1)$, $0 \leq m \leq k-1$

If $n \neq p^{k-1}(p-1)$ then $n \mid p^{k-2}(p-1)$

This implies that $r^{p^{k-2}}(p-1) \equiv 1\left(\bmod p^k\right)$ which contradicts $(\dagger)$

Hence $n = p^{k-1}(p-1)$ i.e. r is a primitive root $\bmod p^k$

□

0.13.10. ***Corollary***

> If p is an odd prime and $k \geq 1$ then there exists a primitive root $\bmod 2p^k$

Proof:

Let r be a primitive root $\bmod p^k$

We may assume that r is odd (or else $r + p^k$ is odd, and is a primitive root $\left(\bmod p^k\right)$)

Let n be the order of $r \bmod 2p^k$

Then $n \mid \phi\left(2p^k\right)$ i.e. $n \mid \phi(2)\phi\left(p^k\right)$ i.e. $n \mid \phi\left(p^k\right)$

However, $r^n \equiv 1\left(\bmod 2p^k\right) \Rightarrow r^n \equiv 1\left(\bmod p^k\right) \Rightarrow \phi\left(p^k\right) \mid n$, since $\phi\left(p^k\right)$ is the order of $r \bmod p^k$

Hence $n = \phi\left(p^k\right) = \phi\left(2p^k\right)$ i.e. r is a primitive root $\bmod 2p^k$

Hence there exists a primitive root $\bmod n$ if and only $n = 2, 4, p^k,$ or $2p^k$ where p is an odd prime.

□

0.13.11. Definition: indices

Suppose that n is an integer for which there exists a primitive root $r \bmod n$

Then if $(a, n) = 1$, then the smallest positive integer k such that $a \equiv r^k (\bmod n)$ is called the index of a relative to r and is written $\text{indr}_r(a)$ or $\text{ind}(a)$ if r is understood

So $1 \leq \text{indr}(r)(a) \leq \phi(n)$ and $r^{\text{ind}_r(n)} \equiv a (\bmod n)$

0.13.12. Example

2 is a primitive root mod 5

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1 (\bmod 5)$

$\therefore \text{Ind}_2(1) = 4, \text{Ind}_2(2) = 1, \text{Ind}_2(3) = 3, \text{Ind}_2(4) = 2$

0.14. Feb 20

We Remind ourselves of the definition of indices

0.14.1. Definition: INdices

Suppose that n is a positive integer for which there exists a primitive root $r \bmod n$

Definition: If $(a, n) = 1$ then the smallest positive integer k such that $a \equiv r^k (\bmod n)$ is called the index of a relative to r and is written $\text{ind}_r(a)$

So

$$1 \leq \text{ind}_r(a) \leq \phi(n)$$

and

$$r^{\text{ind}_r(a)} \equiv a (\bmod n)$$

0.14.2. ***Theorem***

> Suppose that there exists a primitive root $r (\mathrm{mod}\, n)$ then
> (i) $\mathrm{ind}(ab) \equiv \mathrm{ind}(a) + \mathrm{ind}(b) (\mathrm{mod}\, \phi(n))$
> (ii) $\mathrm{ind}\left(a^k\right) \equiv k \cdot \mathrm{ind}(a) (\mathrm{mod}\, \phi(n))$
> (iii) $\mathrm{ind}(1) \equiv 0 (\mathrm{mod}\, \phi(n))$ and $\mathrm{ind}(r) \equiv 1 (\mathrm{mod}\, \phi(n))$

Proof:

(i) $r^{\mathrm{ind}(a)} \equiv a (\mathrm{mod}\, n)$ and $r^{\mathrm{ind}(b)} \equiv b (\mathrm{mod}\, n)$ therefore $r^{\mathrm{ind}(a) + \mathrm{ind}(b)} \equiv ab \equiv r^{\mathrm{ind}(ab)} (\mathrm{mod}\, n)$

Now since the order of $r (\mathrm{mod}\, n)$ is $\phi(n)$ it follows that $\mathrm{ind}(a) + \mathrm{ind}(b) \equiv \mathrm{ind}(ab) (\mathrm{mod}\, \phi(n))$

(ii) $r^{\mathrm{ind}(a^k)} \equiv a^k (\mathrm{mod}\, n)$ then also $\left(r^{\mathrm{ind}(a)}\right)^k \equiv a^k (\mathrm{mod}\, n)$

Hence it follows that $\mathrm{ind}\left(a^k\right) = k \cdot \mathrm{ind}(a) (\mathrm{mod}\, \phi(n))$

(iii) follows by definition

□

0.14.3. Note

An expalation for (ii) above

If $(\alpha, n) = 1$ and $\alpha^m \equiv 1 (\mathrm{mod}\, n)$ then m divides the order of k, of $\alpha (\mathrm{mod}\, n)$ i.e. $m \equiv 0 (\mathrm{mod}\, k)$

So if $\alpha^{m_1} \equiv \alpha^{m_2} (\mathrm{mod}\, n) \Rightarrow \alpha^{m_1 - m_2} \equiv 1 (\mathrm{mod}\, n)$ and so $m_1 - m_2 \equiv 0 (\mathrm{mod}\, k)$ i.e. $m_1 \equiv m_2 (\mathrm{mod}\, k)$

0.14.4. Example

Suppose that there exists a primitive root r mod n and that $(a, n) = 1$

Consider the congruence $x^k \equiv a (\mathrm{mod}\, n) (\dagger)$

This may be rewritten $r^{k \cdot \mathrm{ind}(x)} \equiv r^{\mathrm{ind}(a)} (\mathrm{mod}\, n)$

and so is equivalent to the congruence $k \cdot \mathrm{ind}(x) \equiv \mathrm{ind}(a) (\mathrm{mod}\, \phi(n)) (\star)$

Let $d = (k, \phi(n))$

If $d \nmid \mathrm{ind}(a)$ then $\star$ has no solutions

If $d \mid \mathrm{ind}(a)$ then $\star$ has d solutions

0.14.5. Example

Suppose that $k = 2$, and $n = p$ is an odd prime. Then $(\dagger)$ becomes $x^2 \equiv a (\mathrm{mod}\, p)$ $(\dagger\dagger)$

Then this is equivalent to $2 \cdot \mathrm{ind}(x) \equiv \mathrm{ind}(a) (\mathrm{mod}\, p - 1) (\star\star)$

Since $(2, p - 1) = 2$ then $(\star\star)$ has a solution if and only $2 \mid (\mathrm{ind}(a))$ in which case there are two solutions.

0.14.6. Example

Consider the congruance $4x^9 \equiv 7 (\mod 13) (\dagger)$

Recakk tgat 2 is a primitive root mod 13

$a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ has corresponding idices $\text{ind}_2(a) = 12, 1, 4, 2, 9, 5, 11, 3, 8, 10, 7, 6$

Then $(\dagger)$ has a solution if and only if

$$\text{ind}_2(4) + 9\text{ind}_2(x) \equiv \text{ind}_2(7) (\mod 12) \Rightarrow 9\text{ind}_2(x) \equiv 9 (\mod 12) \Rightarrow 3 \cdot \text{ind}_2(x) \equiv 3 (\mod 4) \Rightarrow \text{ind}_2(x) \equiv 1 (\mod 4)$$

Therefore $\text{ind}_2(x) = 1, 5, \text{or } 9$

Therefore $x \equiv 2, 5, \text{or } 6 (\mod 13)$

0.14.7. *Theorem*

> Let n be an integer such that there exists a primitive root $r (\mod n)$
>
> Suppose that $(a, n = 1)$
>
> Then $x^k \equiv a (\mod n)$ has a solution if and only if
>
> $$a^{\frac{\phi(n)}{d}} \equiv 1 (\mod n) (\star)$$
>
> where $d = (\phi(n), k)$
>
> If this has a solution, then there are exactly d solutions $(\mod n)$

Proof:

Taking indices, we see that $\star$ is equivalent to $\frac{\phi(n)}{d} \text{ind}_r(a) \equiv 0 (\mod \phi(n))$

This holds if and only if $d \mid \text{ind}_r(a)$ i.e. if and only if $x^k \equiv a (\mod n)$ is solvable (from the discussion above)

□

0.14.8. Example

Consider the congruence $x^3 \equiv 4 (\mod 13)$

let $d \coloneqq (3, \phi(13)) = 3$

Therefore $\frac{\phi(13)}{d} = 4$

We have $4^4 = 16 \cdot 16 \equiv 3 \cdot 3 \equiv 9 \not\equiv 1 (\mod 13)$

Therefore the original congruence is not solvable

0.14.9. Example

Consider another congruence $x^3 \equiv 5 (\mod 13) (\dagger)$

WE have $5^4 \equiv 625 \equiv 1 (\mod 13)$ and so $(\dagger)$ has a solution

Note that $(\dagger)$ is equivalent to the congruence $3 \cdot \text{ind}_2(x) \equiv \text{ind}_2(5) (\mod 12)$ i.e. $3\text{ind}_2(x) \equiv 9 (\mod 12) \Rightarrow \text{ind}_2(x) \equiv 3 (\mod 4)$

This last congruence has 3 distinct solutions (mod 12) i.e. $\text{ind}_2(x) \equiv 3, 7, 11 (\mod 12)$

And the corresponding integers are $8, 11, 7$ respectively

So the solutions of $(\dagger)$ are $x \equiv 7, 8, 11 (\mod 12)$

New Topic: quadratic reciprocity law

0.14.10. Remark

Some motivation: suppose that p is an odd prime and consider the congruence $\alpha x^2 + \beta x + \gamma \equiv 0 (\mod p) (\dagger)$ where $(\alpha, p) = 1$

Since p is odd we have $(4\alpha, p) = 1$ and so $(\dagger)$ holds and so $(\dagger)$ yields $4\alpha(\alpha x^2 + \beta x + \gamma \equiv 0 (\mod p)) \Rightarrow (2\alpha x + \beta)^2 - (\beta^2 - 4\alpha\gamma) \equiv 0 (\mod p)$

Say $y = 2\alpha x + \beta, \delta = \beta^2 - 4\alpha\gamma$ then we obtain $y^2 \equiv \delta (\mod p) (\dagger\dagger)$

So

(i) If $x \equiv x_0 (\mod p)$ is a solution of $(\dagger)$ then $y_0 \equiv 2\alpha x_0 + \beta (\mod p)$ is a solution of $(\dagger\dagger)$

(ii) If $y \equiv y_0 (\mod p)$ is a solution of $(\dagger\dagger)$ then we can solve $2\alpha x \equiv y_0 - \beta (\mod p)$ to obtain a solution of $(\dagger)$

So we consider congruence of the form $x^2 \equiv a (\mod p) (\star)$

If $(\star)$ has a solution x_0, then $p - x_0$ is also a solution. These two solutions are distinct $(\mod p)$

0.14.11. Example

Recall Langrange's theorem: If p is a prime and $f(x) = a_n x^n + \ldots + a_0$ where $(a_n, p) = 1$ is a polynomial of degree n with integer coeffeicients thatn $f(x) \equiv 0 (\mod p)$ has at most n distinct solutions $(\mod p)$

Consider the congruence $5x^2 - 6x + 2 \equiv 0 (\mod 13)$ then $\alpha = 5, \beta = -6, \gamma = 2$

Set $\delta = \beta^2 - 4\alpha\gamma = 36 - 40 = -4 \equiv 9 (\mod 13)$

So we consider the congruence $y^2 \equiv 9 (\mod 13)$

This has solutions $y \equiv 3, 10 (\mod 13)$ Next, we solve the linear congruences $10x - 6 \equiv 3 (\mod 13)$ and $10x - 6 \equiv 10 (\mod 13)$ i.e $10x \equiv 9 (\mod 13)$ and $10x \equiv 16 \equiv 3 (\mod 13)$

Check that $x \equiv 10, 12 (\mod 13)$ satisfy these equaitons.

Aim: provide a test for the existence of solutions of the congruence $x^2 \equiv a (\mod p)$ where $(a, p) = 1$ i.e. identify those integers that are perfect squares $(\mod p)$

0.14.12. Definition

Let p be a prime and let a be an integer with $(a, p) = 1$

If $(\star)$ from 0.14.10 has a solution, then a is said to be a quadratic residue mod p

If $(\star)$ from 0.14.10 does not have a solution, then a is said to be a quadratic non-residue mod p

0.15. Feb 25

Last time

0.15.1. Definition: quadratic residue

Let p be an odd prime, and let a be an integer with $(a, p) = 1$

If the congruence $x^2 \equiv a (\mathrm{mod}\, p)$ has a solution, than a is said to be a quadratic residue mod p

If the above congruence has no solution, then a is said to be a quadratic non-residue mod p

Example:

Consider the prime $p = 13$. The quadratic residues mod 13 are $1, 4, 9, 3, 10, 12$ and the quadratic non-residues mod 13 are $2, 5, 6, 7, 8, 11$ (check this!)

0.15.2. Remark

Recall Fermat's little theorem (which is a special case of Euler's theorem)

If p is an odd prime, and a is an integer such that $(a, p) = 1$ then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$

0.15.3. *Theorem:* Euler's criterion

> Suppose that p is an odd prime, and let $a \in \mathbb{Z}$ satisfy $(a,p) = 1$
>
> Then a is a quadratic residue mod p
>
> $$\text{if and only if } a^{(p-1)/2} \equiv 1 (\text{mod}\, p)$$

Proof:

Suppose that a is a quadratic residue mod p such that $x^2 \equiv a (\text{mod}\, p)$

Then $(a,p) = 1$ and raising each side by $\frac{p-1}{2}$ gives us

$$a^{(p-1)/2} \equiv \left(x^2\right)^{(p-1)/2} \equiv x^{p-1} \equiv 1 (\text{mod}\, p)$$

where the last equiv holds by euler's theorem

Conversly, suppose $a^{(p-1)/2} \equiv 1 (\text{mod}\, p)$ Let r be a primitive root mod p

Suppose that $a \equiv r^k (\text{mod}\, p)$ sich that $1 \leq k \leq p$

Then $r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 (\text{mod}\, p)$

Therefore the order of r mod p divides $k(p-1)/2$ i.e. $p-1$ divides $\frac{k(p-1)}{2}$ Hence k is even, with $k = 2j$ then $\left(r^j\right)^2 = r^{2j} = r^k \equiv a (\text{mod}\, p)$ which implies that a is a quadratic residue mod p

□

0.15.4. Remark

Suppose that a, p are as in 0.15.3 above

Then

$$\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) = a^{p-1} - 1 \equiv 0 (\text{mod}\, p)$$

where the last equality holds by Eyler's theorem

Hence either $a^{p-1/2} \equiv 1 (\text{mod}\, p)$ or $a^{(p-1)/2} \equiv -1 (\text{mod}\, p)$ but not both

So if a is a quadratic non-residue mod p then we must have $a^{(p-1)/2} \equiv -1 (\text{mod}\, p)$

0.15.5. *Corollary*

> Let a, p be as above
>
> Then $a^{(p-1)/2} \equiv \{1$ if a is a quadratic residue mod $p; -1$ if a is a quadratic non-residue mod $p\}$

0.15.6. Example

Let $p = 13$ then $2^{(13-1)/2} = 64 \equiv 12 \equiv -1 (\text{mod}\, 13)$ therefore 2 is a quadratic non-residue mod 13

Similarly $3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 (\text{mod}\, 13)$ therefore 3 is a quadratic residue mod 13

0.15.7. *Theorem:* Euler's criterion alternative proof

Suppose that a is a quadratic non-reside mod p, and $c \in \{1, 2, ..., p-1\} := S$

Then there exists a solution $c' \in S$ of the congruence $cx \equiv a (\text{mod } p)$

Since a is a quadratic non-residue mod p we have $c \neq c'$

Therefore the integers in S can be divided into $\frac{p-1}{2}$ pairs $\{c, c'\}$ with $cc' \equiv a (\text{mod } p)$

Therefore we have the congruences (there are $(p-1)/2$) of these:

$$\begin{aligned} c_1 c_{1'} &\equiv a (\text{mod } p) \\ c_2 c_{2'} &\equiv a (\text{mod } p) \\ &\vdots \\ c_{\frac{p-1}{2}} c'_{\frac{p-1}{2}} &\equiv a (\text{mod } p) \end{aligned}$$

Multiplying these congruences together we have

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 (\text{mod } p)$$

where the last equivalence holds by wilson's theorem

Now suppose that a is a quadratic residue mod p

Then the congruence $x^2 \equiv a (\text{mod } p)$ has two solutions: $x = x_1, x = p - x_1$ for $x_1 \in S$

Remove x_1, and $p - x_1$ from S, then the remaining $p-3$ integers can be grouped into pairs c, c' such that $cc' \equiv a (\text{mod } p)$ which gives $\frac{p-3}{2}$ congruences

We also have the congruence $x_1(p - x_1) = x_1 p - x_1^2 \equiv -x_1^2 \equiv -a (\text{mod } p)$
Taking the product of al of these congruences gives:

$$-a^{(p-1)/2} \equiv (p-1)! \equiv -1 (\text{mod } p)$$

i.e. $a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

0.15.8. Definition: Legendre symbol

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

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

if $p \mid a$ we can set $\left(\frac{a}{p}\right) = 0$

For example $\left(\frac{3}{13}\right) = 1, \left(\frac{6}{13}\right) = -1$

0.15.9. *Theorem:* properties of the Legendre symbol

> Let p be an odd prime and let $a, b \in \mathbb{Z}$ with $(a,p) = (b,p) = 1$
> (i) If $a \equiv b (\mathrm{mod}\, p)$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
> (ii) $\left(\frac{a^2}{p}\right) = 1$
> (iii) $\left(\frac{a}{p}\right) \equiv a^{p-1/2} (\mathrm{mod}\, p)$
> (iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
> (v) $\left(\frac{1}{p}\right) = 1$ and $\left(-\frac{1}{p}\right) = (-1)^{p-1/2}$

Proof:

i and ii are clear

(iii): follows from the cololllary to Euler's criterion 0.15.5

(iv): use (iii) above i.e. $\left(\frac{ab}{p}\right) \equiv (ab)^{p-1/2} \equiv a^{p-1/2}\left(b^{p-1/2}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\, p)$

(v) follows from euler's criterion

□

0.15.10. Remark

Observe that $\frac{p-1}{2}$ is even if $p = 4k+1$ and odd if $p = 4k+3$

So

$$-\left(\frac{1}{p}\right) = (-1)^{p-1/2} = \begin{cases} 1 \text{ if } p \equiv 1 (\mathrm{mod}\, 4) \\ -1 \text{ if } p \equiv -1 (\mathrm{mod}\, 4) \end{cases}$$

0.15.11. Example

Determine whether the congruence $x^2 \equiv -46 (\mathrm{mod}\, 17)$ is solvable.

We can evaluate

$$\left(\frac{-46}{17}\right) = \left(-\frac{1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3 \cdot 2^2}{17}\right) = \left(\frac{3}{17}\right) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 (\mathrm{mod}\, 17)$$

So the congruence has no solution (i think by 0.15.8)

0.15.12. *Theorem:* Dirchlet's theorem on primes in an arithmetic progression

> Suppose that $(a,m) = 1$ where $a, m \in \mathbb{Z}_{>0}$, then the arithmetic progression $a, a+m, a+2m, \ldots$ contains infinitely many primes

Proof: outside scope of this course

□

0.15.13. ***Theorem:*** **infinitely many primes of the form** $4k+1$

> There are inifintely many primes of the form 4_1^k

Proof:

Suppose there are only finitely many such primes $p_1, ..., p_n$

Consider the integer $N = (2p_1...p_n)^2 + 1$

Since N is odd, there exists some off prime p where $p \mid N$

i.e. $(2p_1...p_n)^2 \equiv -1 (\mod p) (\dagger)$

So $\left(\frac{-1}{p}\right) = 1$ and therefore $p = 4k+1$ for some k

Hence $p = p_i$ say and now $(\dagger)$ gives $0 \equiv -1 (\mod p_i)$

□

0.16. Feb 27

Law of Quadratic Reciprocity continued

We repeated the definition of the Legendre symbol

0.16.1. ***Theorem***

> Suppose that p is an odd prime, then
>
> $$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$
>
> So there are exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non residues $\mod p$

Proof:

Let r be a primitive root $\mod p$

For any a with $1 \leq a \leq p-1$ there exists a unique k with $1 \leq k \leq p-1$ such that $a \equiv r^k (\mod p)$ Then

$\left(\frac{a}{p}\right) = \left(\frac{r^k}{p}\right) \equiv \left(r^k\right)^{(p-1)/2} \equiv \left(r^{(p-1)/2}\right)^k \equiv (-1)^k (\mod p)$ (euler's crieterion check this TODO)

Note that $r^{(p-1)/2} \equiv -1 (\mod p)$ since r is a primitive root $\mod p$

Hence $\left(\frac{a}{p}\right) = (-1)^k$ since $\left(\frac{a}{p}\right)$ and $(-1)^k$ are both equal to ± 1 We therefore have

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{k=1}^{p-1} (-1)^k = 0$$

□

0.16.2. ***Corollary***

> The quadratic residues mod p (p is odd) are congruent to the even powers of a primitive root mod p while the non-residues are congruent to the odd powers

0.16.3. Example

2 is a primitive root mod 13

Taking the even powers of 2, we have they $2^2 \ldots 2^{12}$ are congruent to $4, 3, 12, 9, 10, 1$ which are the quadratic residues, while if we take odd power of 2 then the quadratic non-residues are $2, 8, 6, 11, 5, 7$

0.16.4. *Lemma:* Gauss's Lemma

Let p be an odd prime, and suppose $a \in \mathbb{Z}$ with $(a,p) = 1$

Let n denote the number of integers in the set $S = \left\{a, 2a, 3a, ..., \frac{p-1}{2}a\right\}$ whose smallest positive residue mod p exceeds $\frac{p}{2}$

Then $\left(\frac{a}{p}\right) = (-1)^n$

Proof:

Consider the set S

Let $\{r_1, ..., r_n\}$ be the set of residues in S that exceed $\frac{p}{2}$

Let $\{s_1, ..., s_n\}$ be the remaining residues in S

Then the r_i and s_j are all distinct, and non-zero, and we have $n + m = \frac{p-1}{2}$

Observe that $0 < p - r_i < \frac{p}{2}$ for $(i - 1, ..., n)$ and the numbers $p - r_i$ are distinct

Claim: no $p - r_i$ is equal to an s_j

First, suppose that $p - r_i = s_j (\star)$

Then $r_i \equiv \rho a (\text{mod}\, p)$ and $s_j \equiv \sigma a (\text{mod}\, p)$ for some $1 \leq \rho, \sigma \leq \frac{p-1}{2}$ and $\rho \neq \sigma$

Thereofre $\star$ implies that $\rho - \rho a \equiv \sigma a \Rightarrow a(\sigma + \rho) \equiv 0 \Rightarrow \sigma + \rho \equiv 0 (\text{mod}\, p)$ which is impossible and proves the claim

So the integers $p - r_1, p - r_2, ..., p - r_n, s_1, s_2, ..., s_m$ are all distinct. They all lie between 1 and $\frac{p-1}{2}$ and there are $\frac{p-1}{2}$ of them. Hence they are just the numbers $1, 2, ..., \frac{p-1}{2}$ in some order.

So

$$(p - r_1)(p - r_2)...(p - r_n)s_1, ...s_m = 1 \cdot 2 \cdot 3...\frac{p-1}{2}$$

$$(-r_1)(-r_2)...(-r_n)s_1, ..., s_m \equiv 1 \cdot 2 \cdot 3...\frac{p-1}{2}$$

$$(-1)^n r_1 r_2 ... r_n s_1 ... s_m \equiv 1 \cdot 2 \cdot 3...\frac{p-1}{2}$$

$$(-1)^n a \cdot 2a ... \frac{p-1}{2}a \equiv 1 \cdot 2 \cdot 3...\frac{p-1}{2}$$

$$(-1)^n \cdot a^{(p-1)/2} \equiv 1$$

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

all modulo p where the very last equivalence holds by Euler's criterion

Note that in the above, it is implied that $\left(\frac{a}{p}\right) = (-1)^n$

□

0.16.5. Example: Gauss's Lemma

let $p = 13$ and $a = 5$ then $(p-1)/2 = 6$ and $S = \{5, 10, 15, 20, 25, 30\}$

modulo 13 S is equivalent to the set $5, 10, 2, 7, 12, 4$ and 3 of these integers exceed $\frac{13}{2}$ (i.e. 10,7,12) therefore $\left(\frac{5}{13}\right) = (-1)^3 = -1$

Note that "residue" has equivalent meaning to "remainder"

We can use Gauss's Lemma to prove serveral interesting results

0.16.6. *Theorem*

> Let p be an odd prime, then
>
> $$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 (\text{mod } 8) \vee p \equiv 7 (\text{mod } 8) \\ -1 \text{ if } p \equiv 3 (\text{mod } 8) \vee p \equiv 5 (\text{mod } 8) \end{cases}$$

Proof:

Let $S = \left\{1 \cdot 2, 2 \cdot 2, 2 \cdot 3, ..., 2 \cdot \frac{p-1}{2}\right\}$

Let n be the number of integers in S that have remainder $> \frac{p}{2}$ when divided by p

Then Gauss's lemma implies that $\left(\frac{2}{p}\right) = (-1)^n$

Since all elements of S are less (mod p) than p , in order to determine n we have to count the number of elements of S which are $> \frac{p}{2}$

If k is such that $1 \leq k \leq \frac{p-1}{2}$ then $2k < \frac{p}{2} \Leftrightarrow k < \frac{p}{4}$

Let [] denote the integer part of some value

Therefore there are [p/4] integers in S less than $\frac{p}{2}$

$\therefore n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$

Now

$$p = 8k + 1 \Rightarrow n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$$

$$p = 8k + 3 \Rightarrow n = 4k + 1 - \left[2k + \frac{3}{4}\right] = 4k + 1 - 2k = 2k + 1$$

similarly, $p = 8k + 5 \Rightarrow n = 2k + 1$ and $p = 8k + 7 \Rightarrow 2k + 2$

So n is even iff $p = 8k + 1$ or $p = 8k + 7$

and n is odd iff $p = 8k + 3$ or $p = 8k + 5$

Therefore

$$\left(\frac{2}{p}\right) = (-1)^n = \begin{cases} 1 \text{ if } p \equiv 1 (\text{mod } 8) \vee p \equiv 7 \text{ mod } 8 \\ -1 \text{ if } p \equiv 3 (\text{mod } 8) \vee p \equiv 5 (\text{mod } 8) \end{cases}$$

□

0.16.7. Remark

If $p = 8k + 1$ i.e. if $p \equiv 1 (\mathrm{mod}\, 8)$ or $p \equiv 7 (\mathrm{mod}\, 8)$ then $\frac{p^2-1}{8} = \frac{(8k\pm)^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$ an even integer

Therefore $(-1)^{(p^2-1)/8} = 1 - \left(\frac{2}{p}\right)$

0.16.8. Remark

If p = 8k + 3 i.e. if $p \equiv 3 (\mathrm{mod}\, 8)$ or $p \equiv 5 (\mathrm{mod}\, p)$ then $\frac{p^2-1}{8} = \frac{(8k\pm 3)^2-1}{8} = 8k^2 \pm 6k + 1$ an odd integer

Therefore $(-1)^{\frac{p^2-1}{8}} = -1 = \left(\frac{2}{p}\right)$

0.16.9. *Corollary*

> If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Took a picture of the last 3 boxes, check

0.17. Mar 4

Last time: Gauss's Lemma

0.17.1. *Theorem*

> Using Gauss's Lemma (last time) we showed that if p is an odd prime, then
>
> $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

0.17.2. *Theorem*

> If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2} \cdot 2$ is a primitive root mod $2p+1$

Proof:

Set $q := 2p+1$

(part a) Suppose that $p \equiv 1 (\mod 4)$. Then $(-1)^{(p-1)/2} \cdot 2 = 2$

Now $\phi(q) = q - 1 = 2p$

Therefore the order of $2 \bmod p$ is $1, 2, p,$ or $2p$

We have $\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \bmod (q) \equiv 2^p (\mod q)$ by euler's crieterion

But $q = 2p+1$ so $q \equiv 3 (\mod 8)$ therefore $\left(\frac{2}{q}\right) = -1$ and $2^p \equiv -1 (\mod q)$

and we can see the 2 does not have order $p \bmod q$

Next, observe that also if $2^2 \equiv 1 (\mod q)$ then $q \mid 3$ which is a contradiction. Therefore the order or 2 mod q is $2p$ i.e. 2 is a primitive root mod q

(part b) Suppose that $p \equiv 3 (\mod 4)$ then $(-1)^{(p-1)/2} \cdot 2 = -2$

We have $(-2)^p = (-2)^{(q-1)/2} \equiv \left(-\frac{2}{q}\right) (\mod q) \equiv \left(-\frac{1}{q}\right)\left(\frac{2}{q}\right) (\mod q)$

Now $q = 2p+1$ and so $q \equiv 7 (\mod 8)$

Hence $\left(-\frac{1}{q}\right) = -1$ and $\left(\frac{2}{q}\right) = 1$ hence $(-2)^p \equiv -1 (\mod q)$

Now we conclude as before that -2 is a primitive root mod q

□

0.17.3. Remark

It is not known whether there are infinitely many primes p such that $2p+1$ is also prime (called "Sophie Germain primes")

0.17.4. *Theorem*

> There are infinitely many primes of the form $8k-1$

Proof:

Suppose that there are only finitely many such primes $p_1, ..., p_n$ and set $N = (4p_1 ... p_n)^2 - 2$

Since $\frac{N}{2}$ is odd, N is divisble by an odd prime p

This implies that $2 \equiv (4p_1, ..., p_n)^2 (\mod p)$ and so $\left(\frac{2}{p}\right) = 1$ and hence $p \equiv \pm 1 (\mod 8)$

If all prime divisors of N are of the form $8k+1$ then N would be of the form $8\alpha + 1$. This would be a contradiction since N is of the form $16\alpha - 2$

Therefore N has a prime divisor q of the form $8k-1$

Therefore $q \mid N$ and $q \mid (4p_1 ... p_n)^2$ and $q \mid 2$ which is a contradiction. The claim follows.

□

We will need the following result in the proof of the law of quadratic reciprocity

0.17.5. ***Theorem***

> Suppose that p is an odd prime, and a is an odd integer
>
> Then $\left(\frac{a}{p}\right) = (-1)^t$ where
>
> $$t = \sum_{j=1}^{p-1/2} \left[\frac{ja}{p}\right]$$

Proof:

We use the same notation as in the proof of Gauss's Lemma: $S = \left\{a, 2a, ..., \frac{p-1}{2}a\right\}$

$\{r_1, ..., r_n\}$ is the set of residues of elements in S that exceed $\frac{p}{2}$ and $\{s_1, ..., s_m\}$ are the remaining residues

Dividing each of the integers ka by p yields $ka = q_k p + t_k$ for $1 \leq t_k \leq p-1 \Rightarrow \frac{ka}{p} = q_k + \frac{t_k}{p} \Rightarrow q_k = \left[\frac{ka}{p}\right]$

Hence for $1 \leq k \leq (p-1)/2$ we have $ka = \left[\frac{ka}{p}\right]p + t_k$ $(\dagger)$

If $t_k > \frac{p}{2}$ then t_k is one of the integers $r_1, ..., r_n$

If $t_k < \frac{p}{2}$ then t_k is one of the integers $s_1, ..., s_m$

Therefore taking the sum of the equations $(\dagger)$ gives

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right]p + \sum_{k=1}^{n} r_k + \sum_{k=1}^{m} s_k (*)$$

Now from the proof of Gauss's Lemma the $(p-1)/2$ integers $p - r_1, p - r_2, ..., p - r_n, s_1, ..., s_m$ is some rearrangement of the integers $1, 2, ..., \frac{p-1}{2}$

So

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{n}(p - r_k) + \sum_{k=1}^{m} s_k = pn - \sum_{k=1}^{n} r_k + \sum_{k=1}^{m} s_k (\dagger\dagger)$$

Subtracting $(\dagger\dagger)$ from $(*)$ yields $(a-1)\sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k-1}^{(p-1)/2} -n\right) + 2\sum_{k=1}^{n} r_k (\dagger\dagger\dagger)$

Observe that $p \equiv a \equiv 1 (\mathrm{mod}\, 2)$ So $(\dagger\dagger\dagger)$ yields

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] - n\right) + 0 (\mathrm{mod}\, 2) \Rightarrow n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p}\right] (\mathrm{mod}\, 2)$$

And the result follows from Gauss's Lemma:

$\left(\frac{a}{p}\right) = (-1)^n = (-1)^t$

□

0.17.6. Example:

Example $p = 13$ and $a = 5$ since $\frac{p-1}{2} = 6$ we calculate $\left[\frac{ka}{p}\right]$ for $k = 1, 2, ..., 6$

$\left[\frac{5}{13}\right] = \left[\frac{10}{13}\right] = 0$

$\left[\frac{15}{13}\right] = \left[\frac{20}{13}\right] = \left[\frac{25}{13}\right] = 1$

$\left[\frac{30}{13}\right] = 2$

We can observe that $\left(\frac{5}{13}\right) = (-1)^{1+1+1+2} = (-1)^5 = -1$

0.17.7. *Theorem*

> Suppose that p, q are distinct odd primes. Then
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Proof:

Let R denote the rectangle (not including the boundary) in the xy plane with vertices $(0,0)(\frac{p}{2},0)(0,\frac{q}{2}),(\frac{p}{2},\frac{q}{2})$

□

0.18. March 6

0.18.1. ***Theorem:*** **The Law of Quadratic Reciprocity**

> Suppose that p, q are distinct odd primes. Then
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Proof:

Let R denote the rectangle (not including the boundary) in the xy plane whose vertices are $(0,0)(\frac{p}{2},0)(0,\frac{q}{2}),(\frac{p}{2},\frac{q}{2})$

Aim: count the number of lattice points (i.e. points with integer coordinates) in two different ways.

1st way: Since p, q are both odd, the lattic points in R consist of all points (n, m) with $1 \leq n \leq \frac{p-1}{2}$ and $1 \leq m \leq \frac{q-1}{2}$

Therefore the total number of such points is $\frac{p-1}{2} \cdot \frac{q-1}{2}$

2nd way: Let D denote the diagonal from $(0,0)$ to $(\frac{p}{2},\frac{q}{2})$

Aim: count the number of lattice points above D and below D

Claim: None of the lattice points in R lies on D

The equation of D is $y = \frac{q}{p}x$ i.e. $py = qx(\dagger)$

Suppose that (x_1, y_1) is a lattice point on D. Then $(\dagger)$ implies that $py_1 = qx_1$. But since p and q are coprime, this implies that $p \mid x_1$ and $q \mid y_1$, therefore there are no such points in R

Therefore for $1 \leq k \leq (p-1)/2$ there are exactly $\left[\frac{kq}{p}\right]$ lattice points in T_1 directly above $(k,0)$ and below D_1 (these points lie on the vertical line segment from $(k,0)$ to $\left(k, \frac{kq}{p}\right)$) where T_1 is the region below the diagonal

Therefore the total number of lattice points in $T_1 = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]$

A similar calculation (interchanging the roles of p and q) show that the total number of lattic points in (above the diagonal) $T_2 = \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]$

Therefore we have

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right] + \sum_{j=1}^{(p-1)/2} \left[\frac{jq}{p}\right]$$

Now, we showed earlier that $\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right]}$ and $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{kq}{p}\right]}$

Therefore wethe claim holds

□

0.18.2. ***Corollary***

> If p, q are distinct odd primes then
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 (\mod 4) \vee q \equiv 1 (\mod 4) \\ -1 \text{ if } p \equiv q \equiv 3 (\mod 4) \end{cases}$$

Proof:

Observe that $\frac{p-1}{2}\frac{q-1}{2}$ is even if and only if at least one of p, q is of the form $4k+1$. If both are of the form $4k+3$, then $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is odd. (look at the quadratic reciprocity)

□

0.18.3. ***Corollary***

> If p, q are distinct odd primes, then
>
> $$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) \text{if } p \equiv 1 (\mod 4) \vee q \equiv 1 (\mod 4) \\ -\left(\frac{q}{p}\right) \text{ if } p \equiv q \equiv 3 (\mod 4) \end{cases}$$

Proof:

by the corollarly 0.18.2

□

0.18.4. Example

Consider the Legendre symbol $\left(\frac{29}{53}\right)$

We have $29 \equiv 1 (\mod 43)$ and $53 \equiv 1 (\mod 4)$ so $\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{4}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$

Now since $\left(\frac{2}{29}\right) = -1$ since $29 \equiv 5 (\mod 8)$

and $\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1$

and we have that $\left(\frac{29}{53}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = 1$

0.18.5. Example:

Modulo which primes p where $p \neq 3$ is 3 a quadratic residue?

Answer: apply quadratic reciprocity law:

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) \text{ if } p \equiv 1 (\text{mod } 4) \\ -\left(\frac{p}{3}\right) \text{ if } p \equiv 3 (\text{mod } 4) \end{cases}$$

Nowe we have $p \equiv 1 (\text{mod } 3)$ or $p \equiv 2 (\text{mod } 3)$ We can see easily that

$$\left(\frac{p}{3}\right) = \{1 \text{ if } p \equiv 1 (\text{mod } 3), -1 \text{ if } p \equiv 2 (\text{mod } 3)\}$$

Hence $\left(\frac{3}{p}\right) = 1$ iff either $p \equiv 1 (\text{mod } 4) \wedge p \equiv 1 (\text{mod } 3) (\dagger)$ or $p \equiv 3 (\text{mod } 4) \wedge p \equiv 2 (\text{mod } 3) (\dagger\dagger)$

$(\dagger)$ holds iff $p \equiv 1 (\text{mod } 12)$ and

$(\dagger\dagger)$ holds iff $p \equiv 11 (\text{mod } 12)$ i.e $p \equiv -1 (\text{mod } 12)$

So we deduce that if $p \neq 3$ is an odd prime, then $\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 (\text{mod } 12) \\ -1 \text{ if } p \equiv \pm 5 (\text{mod } 12) \end{cases}$

0.18.6. Definition: The Jacobi Symbol

Let Q be a positive odd integer, so that $Q = q_1, ..., q_s$ (note that q_i are odd and not necessarily distinct primes)

Suppose $P \in \mathbb{Z}$ with $(P, Q) = 1$ The jacobi symbol $\frac{P}{Q}$ is defined by

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{s} \left(\frac{P}{q_i}\right)$$

where $\left(\frac{P}{q_i}\right)$ is the legendere symbol

0.18.7. Remark

P is a quadratic residue mod Q implies that P is a quadratic residue mod each q_j implies that $\left(\frac{P}{q_j}\right) = 1$ for each j implies $\left(\frac{P}{Q}\right) = 1$

0.18.8. Remark

However, $\left(\frac{P}{Q}\right) = 1$ does not imply that P is a quadratic residue mod Q

For example, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$

But $x^2 \equiv 2 (\text{mod } 15)$ has no solution

0.18.9. Remark

If Q is odd, then a is a quadratic residue mod Q iff $\left(\frac{a}{p}\right) = 1$ for every prime p dividing Q

Therefore $\left(\frac{a}{Q}\right) = -1$ implies that a is a quadratic nonresidue mod Q

For example, $\left(\frac{6}{35}\right) = \left(\frac{6}{5}\right)\left(\frac{6}{7}\right) = \left(\frac{1}{5}\right)\left(-\frac{1}{7}\right) = -1$ so 6 is a quadratic non-residue mod 35

0.18.10. ***Theorem***

Suppose that Q, Q' are odd and positive. Then

(i)

$$\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$$

(ii)

$$\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$$

(iii) if $(P, Q) = 1$ then

$$\left(\frac{P^2}{Q}\right) = \left(\frac{Q}{P^2}\right) = 1$$

(iv) If $(PP', QQ') = 1$ then

$$\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$$

(v) If $P \equiv P' (\mathrm{mod}\, Q)$ then

$$\left(\frac{P'}{Q}\right) = (PQ)$$

Proof:

(i) follows from the definition of $\left(\frac{P}{Q}\right)$

(ii) Follows from (i) and the multiplicativity of the legendre symbol

(iii) Follows from (i, and ii)

(iv) Follows from (ii and i)

(v) Set $Q = q_1 ... q_s$ then $P \equiv P' \left(\mathrm{mod}\, q_j\right)$ so $\left(\frac{P'}{q_j}\right) = \left(\frac{P}{q_j}\right)$ and deduce the result from this

□

0.19. March 11

The Jacobi symbol continued

0.19.1. Definition

Suppose that Q is an odd positive integer with $Q = q_1 ... q_s$ (where q_i are not necessarily distinct primes)

suppose $P \in \mathbb{Z}$ with $(P, Q) = 1$

then we define the jacobi symbol $\left(\frac{P}{Q}\right)$ as $\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$ where $\left(\frac{P}{q_j}\right)$ is the legendere symbol

0.19.2. *Theorem*

If Q is odd, and $Q > 0$ then $\left(-\frac{1}{Q}\right) = (-1)^{(Q-1)/2}$ and $\left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$

Proof:

$$\left(-\frac{1}{Q}\right) = \prod_{j=1}^{s} \left(\frac{p}{q_j}\right) = \prod_{j=1}^{s} (-1)^{(q_j-1)/2} = (-1)^{\sum_{j=1}^{s} (q_j-1)/2}$$

Now observe that if a, b are odd then

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 (\mathrm{mod}\, 2)$$

and so

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} (\mathrm{mod}\, 2)$$

Applying this repeately gives

$$\sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{1}{2}\left(\left[\prod_{j=1}^{s} q_j\right] - 1\right) \equiv \frac{Q-1}{2} (\mathrm{mod}\, 2)$$

Hence $\left(-\frac{1}{Q}\right) = (-1)^{(Q-1)/2}$

Similarly, if a, b are odd then

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 (\mathrm{mod}\, 2)$$

and so $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} (\mathrm{mod}\, 2)$

Therefore $\left(\frac{2}{Q}\right) = \prod_{j=1}^{s} \left(\frac{2}{q_j}\right) = (-1)^{\sum_{j=1}^{s} (q_j^2-1)/8} = (-1)^{(Q^2-1)/8}$

□

0.19.3. ***Theorem***

> If P, Q are odd and positive, and $(P, Q) = 1$ then $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{P-\frac{1}{2}Q-\frac{1}{2}}$

Proof:

Use law of quadratic reciprocity

Set $P = \sum_{i=1}^{r}(p_i)$ and $Q = \prod_{j=1}^{s} q_j$

Then

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \left(\frac{Q}{P}\right)\cdot(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

Now just as before $\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{p-1}{2} \pmod 2$ and $\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{Q-1}{2} \pmod 2$ Hence $\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)\cdot(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$

□

0.19.4. Remark

If we try to define

$$\left(\frac{P}{Q}\right) = \begin{cases} +1 \text{ if } P \text{ is a quadratic residue mod } Q \\ -1 \text{ if } P \text{ is a quadratic non-residue mod } Q \end{cases}$$

then we lose the reciprocity law e.g. Take $P = 5$ and $Q = 9$

0.19.5. Example

Using Jacobi symbols can sometimes helps us evaluate legendre symbols

For example $\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1$ where the first equlaity holds by the "quadratic reciprocity" of Jacobi symbols

So 105 is a quadratic residue modulo 317

0.19.6. Example

Consider the congruence $x^2 \equiv 196 (\mathrm{mod}\, 1357) (\dagger)$

Since $1357 = 23 \cdot 59$ then $(\dagger)$ is soluble if and only if both $x^2 \equiv 196 (\mathrm{mod}\, 23)$ and $x^2 \equiv 196 (\mathrm{mod}\, 59)$ are soluble

So we evaluate $\left(\frac{196}{23}\right)$ and $\left(\frac{196}{59}\right)$

Firstly, $\left(\frac{196}{23}\right) = \left(\frac{12}{23}\right) = \left(\frac{3}{23}\right) = 1$ and secondly, $\left(\frac{196}{59}\right) = \left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right) = -\left(\frac{2}{19}\right) = -(-1) = 1$ so $(\dagger)$ can be solved

How do we find the solutions?

Note that $x^2 \equiv 196 \equiv 12 (\mathrm{mod}\, 23)$ is satisfied by $x \equiv 9, 14 (\mathrm{mod}\, 23)$

$x^2 \equiv 196 \equiv 19 (\mathrm{mod}\, 59)$ is satisfied by $x \equiv 14, 45 (\mathrm{mod}\, 59)$

Now we use the Chinese remainder theorem to obtain the simultaneous solutions of the following systems of congruences:

$x \equiv 14 (\mathrm{mod}\, 23)$ and $x \equiv 14 (\mathrm{mod}\, 59)$

$x \equiv 14 (\mathrm{mod}\, 23)$ and $x \equiv 45 (\mathrm{mod}\, 59)$

$x \equiv 9 (\mathrm{mod}\, 23)$ and $x \equiv 14 (\mathrm{mod}\, 59)$

$x \equiv 9 (\mathrm{mod}\, 23)$ and $x \equiv 45 (\mathrm{mod}\, 59)$

The answers are $x \equiv 14, 635, 722, 1345 (\mathrm{mod}\, 1357)$ (note that these answers given by the professor may be wrong)

quadratic congruences with composite moduli

0.19.7. *Theorem*

> Suppose that p is an odd prime and $a \in \mathbb{Z}$ with $(a, p) = 1$
>
> Then $x^2 \equiv a (p^n)$ for $n \geq 1$ $(\star)$
>
> is solvable if and only if $\left(\frac{a}{p}\right) = 1$

Proof: Plainly if $(\star)$ is soluble so is $x^2 \equiv a (\mathrm{mod}\, p)$ whence (therefore) $\left(\frac{a}{p}\right) = 1$

Now suppose that $\left(\frac{a}{p}\right) = 1$ and use induction on n

Assume that the result holds for $n = k \geq 1$ i.e. that $x^2 \equiv a\left(p^k\right)$ admits a solution x_0 Then $x_0^2 = a + bp^k$ for some b

Now consider the congruence $2x_0 y \equiv -b (\mathrm{mod}\, p)$: this has a unique solution $y \equiv y_0 (\mathrm{mod}\, p)$ (say)

Now consider the integer $x_1 = x_0 + y_0 p^k$

We have $x_1^2 = \left(x_o + y_0 p^k\right)^2 = x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k} \equiv a + (b + 2x_0 y_0) p^k + y_0^2 p^{2k}$

But $p \mid (b + 2x_0 y_0)$ and so $x_1^2 \equiv a\left(p^{k+1}\right)$

□

0.19.8. ***Theorem***

> Suppose that a is an odd integer
>
> (i) $x^2 \equiv a (\mod 2)$ always has a solution
>
> (ii) $x^2 \equiv a (\mod 4)$ has a solution if and only if $a \equiv 1 (\mod 4)$
>
> (iii) For $n \geq 3$ then $x^2 \equiv a (\mod 2^n)$ has a solution if and only if $a \equiv 1 (\mod 8)$

Proof:

(i) and (ii) are "easy"

for (iii):

If $x^2 \equiv a (\mod 2^n)$ and $n \geq 3$ has a solution, becasue the square of any odd integer is congruent to $1 \bmod 8$

i.e. $(4k \pm 1)^2 = 16k^2 \pm 8k + 1 \equiv 1 (\mod 8)$

Fix a value of $n \geq 3$ and assume that $x^2 \equiv a (\mod 2^n)$ has a solution x_0

So $x_0^2 = a + b2^n$ for some b where a is odd (therefore x_0 is odd also)

Consider the congruence $x_0 y \equiv -b (\mod 2)$

This has a unique solution $y \equiv y_0 (\mod 2)$ say Now look at the integer $x_1 = x_0 + y_0 2^{n-1}$

Therefore $x_1^2 = \left(x_0 + y_0 2^{n-1}\right)^2 = x_0^2 + x_0 y + 02^n + y_0^2 \cdot 2^{2n-2} = a + (b + x_0 y_0) 2^n + y_0^2 2^{2n-2}$

Now $2 \mid (b + x_0 y_o)$ and $2n - 2 = n + 1 - (n - 3) > n + 1$

Therefore $x_1^2 = \left(x_0 + y 2^{n-1}\right)^2 \equiv a (\mod 2^{n+1})$

Look up p-adic numbers

TODO: fill in (took a picture)

□