1 Mon 9/28

Quick recap of Fermat's Little Theorem and Euler's Theorem:

Fermat

Let p be a prime. Let $a \in \mathbb{Z}$ such that $\gcd(a, p) = 1$. Then

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

Euler

A generalization of Fermat's Little Theorem: Let $m \geqslant 2$ be an integer. Let $a \in \mathbb{Z}$ with $\gcd(a, m) = 1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Since Euler's Theorem is far stronger than Fermat's ($\varphi(p) = p - 1$ if p is a prime), we will only give a proof for Euler's.

Proof: Euler

Let r be the remainder when a is divided by m. Then $o \leqslant r \leqslant m - 1$. Since $\gcd(a, m) = 1$, we see that r cannot be 0 or any element not coprime to m. In other words,

$$r \in (\mathbb{Z}/m\mathbb{Z})^*.$$

We know that $((\mathbb{Z}/m\mathbb{Z})^*, \times \pmod{m})$ is a group of size $\varphi(m)$. Therefore $o(r)$, by Lagrange's theorem, divides $\varphi(m)$. Hence $r^{\varphi(m)} = 1$, and so is $a^{\varphi(m)}$. □

Structure of group $(\mathbb{Z}/m\mathbb{Z}, +)$

Example 1.1

Consider the group $\mathbb{Z}/6\mathbb{Z}$ under addition. Clearly 0 is not a generator since $0 + 0 + \cdots = 0$. Equally clear is that 1 is a generator. 2 is not because it can only generate multiples of 2. Likewise 3 is not.

In general, there are $\varphi(m)$ generators for this group again because the congruence relation

$$ax \equiv b \pmod{m}$$

is always solvable only when $\gcd(a,m) = 1$. Therefore a can be a generator only when $\gcd(a.m) = 1$, and there are $\varphi(m)$ such a's.

More abstractly, when is an element $a \in (G, \cdot)$ a generator?

Definition 3

Given group $(G, \cdot)$ and an element a of the group, we say a is a **generator** if and only if

$$\{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\} = G.$$

Remark

It is *not* true that every group must have a generator. Consider the group $\mathbb{Z}/8\mathbb{Z}$ under multiplication. Odd elements cannot generate even elements and vice versa.

A group with a generator is called a **cyclic group**.

Example 1.2

Consider G a finite group. Suppose $o(g) = 3$. What is $o(g^2)$?

Solution

Obviously $o(g^2) = 3$ because $(g^2)^3 = g^6 = (g^3)^2 = e$ while g^2, g^4 are not units.

Remark

More generally, if $o(g) = m$, then $o(g^k) = m/\gcd(m,k)$. This has been shown already since we are looking for the smallest integer x satisfying $m \mid kx$.

Example 1.3

If $|G| = 3$ and $o(g) = 1$, is g a generator? What if $o(g) = 2$? What if $o(g) = 3$?

Solution

Clearly if $o(g) = 1$ then g is the unit and is not the generator. If $o(g) = 2$ then it can only generate two elements and hence not G. If $o(g) = 3$ then $\langle g \rangle = \{g, g^2, g^3\}$ which has order 3 (check g, g^2, g^3 are distinct).

Remark

If a finite group G has order m, then g is a generator if and only if $o(g) = m$.

2 Wed 9/30

Lemma 2.1

Suppose $|G| = m$. Then $g \in G$ is a generator if and only if $o(g) = m$.

Proof

We first show $\Longleftarrow$: assume $o(g) = m$, then

$$g^m = e \text{ and } g^i \neq e \text{ for all } 1 \leqslant i \leqslant m-1,$$

and

$$g^i \neq g^j \text{ for all } 0 \leqslant i < j \leqslant m-1$$

because if they were equal, we have $e = g^{j-i}$ by cancellation law, but that's absurd. Then,

$$\{g^0, g^1, \dots, g^{m-1}\}$$

is a set with m distinct elements. Since $|G| = m$, we have already produced all elements of G. Hence it is generated by g.

Now for $\Longrightarrow$. Assume $g \in G$ is a generator. Then we know $|G| = m$ and so $o(g)$ is finite. Let $o(g) = k$, then $g^{-1} = g^{k-1}$. Therefore

$$\{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\} = \{e, g, g^2, \dots\}.$$

By the division algorithm, we also know that $g^n = g^{qk+r}$ where $0 \leqslant r \leqslant k-1$. Hence $g^n = g^r$ with $0 \leqslant r \leqslant k-1$.

Hence

$$\{e, g, g^2, \dots\} = \{e, g, g^2, \dots, g^{k-1}\}.$$

Since we know $|G| = m$ and this set has k distinct elements, we conclude that $k = m$. □

3 Fri 10/2: Computing $\varphi(m)$

Consider $\varphi(12), \varphi(3)$, and $\varphi(4)$. Clearly,

$$\begin{aligned} \varphi(12) = |(\mathbb{Z}/12\mathbb{Z})^*| &= \{1, 7, 9, 11\} \\ \varphi(4) = |(\mathbb{Z}/4\mathbb{Z})^*| &= \{1, 3\} \\ \varphi(3) = |(\mathbb{Z}/3\mathbb{Z})^*| &= \{1, 2\} \end{aligned}$$

By the definition $A \times B = \{(a, b) \mid a \in A, b \in B\}$, we have

$$|A|, |B| < \infty \implies |A \times B| = |A||B|.$$

If we enumerate the elements of $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^*$, we get

$$(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* = \{(1, 1), (1, 3), (2, 1), (2, 3)\}.$$

Now consider the mapping from $(\mathbb{Z}/12\mathbb{Z})^* \to (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^*$ by

$$[a]_{12} \mapsto ([a]_3, [a]_4)$$

More generally, if m and n are co-prime, the function $f : (\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ defined by

$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

is a bijection. Hence $\varphi(mn) = \varphi(m)\varphi(n)$. (Easy to verify that this is a bijection if we verify the injectivity and surjectivity respectively.)

Remark

Now suppose for some huge number k we can [by Fundamental Theorem of Algebra] prime factorize it as the product $p_1^{e_1} p_2^{e_2} \dots p_\ell^{e_\ell}$ where p_i's are prime factors. (For example $9009 = 3^2 \cdot 7 \cdot 11 \cdot 13$.) Clearly $p_1^{e_1}$ is only divisible by powers of p_1, $p_2^{e_2}$ by powers of p_2, etc. It follows that these $(p_i^{e_i})$'s are pairwise coprime to each other.

Recall that if m, n are coprime, then the function $f : (\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ defined by

$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

is a bijection in the sense that, if m, n are coprime, then the system of congruences

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}$$

has precisely one (not more, not fewer) solution between 0 and $(mn) - 1$. (This is guaranteed by the Chinese remainder theorem I think, but it's not hard to verify anyway.)

So, there exists a one-to-one correspondence between elements in $(\mathbb{Z}/mn\mathbb{Z})^*$ and $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. This suggests that the two sets "are equally large" or "contain same amount of elements". Then

$$|(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*||(\mathbb{Z}/n\mathbb{Z})^*| \implies \varphi(mn) = \varphi(m)\varphi(n).$$

Coming back to the huge number k, if follows that, since the $(p_i^{e_i})$'s are pairwise coprime,

$$\varphi(k) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})\dots\varphi(p_\ell^{e_\ell}).$$

Now we want to compute $\varphi(p_i^{e_i})$ for each term, and the question becomes, given a prime p raised to some power p^e, what is the order of $(\mathbb{Z}/p^e\mathbb{Z})^*$, or what is $\varphi(p^e)$ (how many numbers between 1 and p^e are co-prime to p^e)? Clearly any number that aren't multiples of p is co-prime to p^e [why?], and there are p^e/p such numbers between 1 and p^e. Hence if we exclude these numbers we see that

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

(Example: $\varphi(125) = 125 - 25 = 100$ because there are 100 numbers between 1 and 125 that's not a multiple of 5 and hence coprime to 125.)

Therefore,

$$\begin{aligned}\varphi(k) &= \varphi(p_1^{e_1})\varphi(p_2^{e_2})\dots\varphi(p_\ell^{e_\ell})\\ &= \left[p_1^{e-1}\left(1 - \frac{1}{p_1}\right)\right]\left[p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\right]\dots\left[p_\ell^{e_\ell}\left(1 - \frac{1}{p_\ell}\right)\right]\\ &= (p_1^{e_1}p_2^{e_2}\dots p_\ell^{e_\ell})\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_\ell}\right)\\ &= k\prod_{i=1}^{\ell}\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

Quick example: **for the last problem on HW 3/4**, $229 - 1 = 228 = 2^2 \cdot 3 \cdot 19$ so

$$\varphi(228) = 228 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{18}{19} = 72,$$

which is precisely the number of generators of $(\mathbb{Z}/229\mathbb{Z})^*$.

Theorem: Evaluating Euler's Totient Function

Suppose $n \in \mathbb{N}$ has prime factorization $n = \prod_{i=1}^{\ell} p_i^{e_i} = p_1^{e_1}p_2^{e_2}\dots p_\ell^{e_\ell}$, then

$$\varphi(n) = n \cdot \prod_{i=1}^{\ell}\left(1 - \frac{1}{p_i}\right).$$

4 Mon 10/5

Definition 5

$f : \mathbb{Z} \to \mathbb{Z}$ is said to be **multiplicative** if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

The remark above shows that φ is multiplicative.

5 Wed 10/7

A more interesting theorem about $\varphi(n)$:

Theorem 6

Let $N \geqslant 2$. We have

$$N = \sum_{d \geqslant 1 \mid N} \varphi(d).$$

In other words, N is the sum of $\varphi(d)$ for all divisors $d \mid N$.

Example 5.1

Take $N = 12$. We can partition $\{1, 2, \ldots, 12\}$ into sets of numbers coprime to 12, set of numbers with $\gcd = 2$ with 12, with 3, with 4, with 6, and with 12. Then

$$\{1, 2, \ldots, 12\} = \{1, 5, 7, 11\} \sqcup \{2, 10\} \sqcup \{3, 9\} \sqcup \{4, 8\} \sqcup \{6\} \sqcup \{12\}$$

The first set has cardinality $\varphi(12)$, the second $\varphi(6)$, the third $\varphi(4)$, the other three $\varphi(3), \varphi(2), \varphi(1)$. (Think of the second set as the set of numbers of form $2n$ where $\gcd(n, 6) = 1$; 6 comes from $12/2$.) Notice that we originally partitioned the set by different gcd's, and what we get are sets with cardinality $N/\gcd$.

6 Fri 10/9

Fundamental Theorem of Arithmetic, FTA

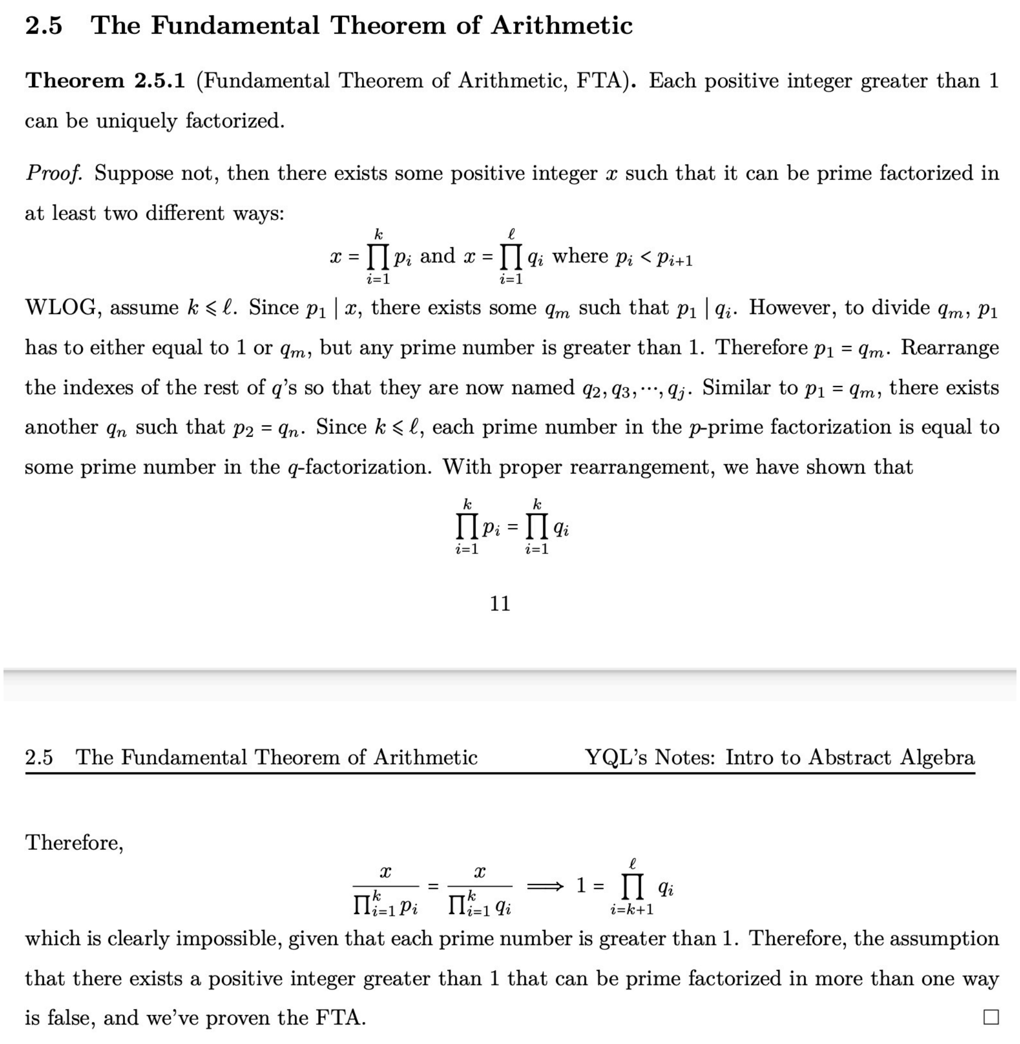
Each positive integer greater than 1 can be uniquely factorized.

Proof

First we show that each number can be prime factorized. Suppose not, then

$$S := \{x \in \mathbb{N} \mid x \geqslant 2 \text{ and } x \text{ does not have prime factors}\}$$

is not empty and thus have a least element m by the well-ordering axiom. Since m cannot be a prime, $m = ab$ for some composite numbers, but a and b can be written as product of primes. Hence m can be written as primes, contradiction. Now for the uniqueness:



2.5 The Fundamental Theorem of Arithmetic

Theorem 2.5.1 (Fundamental Theorem of Arithmetic, FTA)**.** Each positive integer greater than 1 can be uniquely factorized.

Proof. Suppose not, then there exists some positive integer x such that it can be prime factorized in at least two different ways:

$$x = \prod_{i=1}^{k} p_i \text{ and } x = \prod_{i=1}^{\ell} q_i \text{ where } p_i < p_{i+1}$$

WLOG, assume $k \leqslant \ell$. Since $p_1 \mid x$, there exists some q_m such that $p_1 \mid q_i$. However, to divide q_m, p_1 has to either equal to 1 or q_m, but any prime number is greater than 1. Therefore $p_1 = q_m$. Rearrange the indexes of the rest of q's so that they are now named $q_2, q_3, \cdots, q_j$. Similar to $p_1 = q_m$, there exists another q_n such that $p_2 = q_n$. Since $k \leqslant \ell$, each prime number in the p-prime factorization is equal to some prime number in the q-factorization. With proper rearrangement, we have shown that

$$\prod_{i=1}^{k} p_i = \prod_{i=1}^{k} q_i$$

Therefore,

$$\frac{x}{\prod_{i=1}^{k} p_i} = \frac{x}{\prod_{i=1}^{k} q_i} \implies 1 = \prod_{i=k+1}^{\ell} q_i$$

which is clearly impossible, given that each prime number is greater than 1. Therefore, the assumption that there exists a positive integer greater than 1 that can be prime factorized in more than one way is false, and we've proven the FTA. □

□

Example 6.1

Are there infinitely many primes 3 mod 4?. Yes. Suppose not, and suppose $\{p_1, \dots, p_n\}$ exhausts all primes 3 mod 4. Then

$$N = 2p_1p_2 \dots p_n + 1$$

is either $2 \cdot 1 + 1$ or $2 \cdot (-1) + 1$ mod 4, but both are 3. Notice that N is odd. Suppose it were the product of some primes then

$$N = q_1q_2 \dots q_n$$

and reducing both sides module 4 gives

$$3 = [q_1][q_2] \dots [q_n].$$

Notice that [1] has no effect on the right hand side, so if N were a multiple of primes, there must be some q_i's that are 3 mod 4 because it's impossible to get [3] out of a bunch of [1]'s. But we've shown that N is not a multiple of any prime of form $4k + 3$, contradiction.

Remark

There are also infinitely many primes of form $4k + 1$.

Dirichlet's Theorem

If a, b are positive coprime integers, then the sequence

$$(a, a + b, a + 2b, \dots)$$

has infinitely many primes. *Proof is beyond the scope.*

Remark

By this theorem, the sequences $(3, 7, 11, \dots)$ and $(1, 5, 9, \dots)$ both contain infinitely many primes.

7 Mon 10/12

Though we are not going to prove Dirichlet's Theorem, we can make some connections between it and some special cases:

(1) Let $a = b = 1$, then the sequence $(1, 2, \dots)$ has infinitely many primes: *there are infinitely primes.*

(2) Let $a = 3$, $b = 4$, or $a = 1$, $b = 4$, then we see that there are infinitely many primes of form $4k + 1$ and also infinitely many primes of form $4k + 3$.

Theorem 9

There are infinitely many primes that are 1 mod 4.

Proof

We will prove by contradiction. Suppose there were only finitely many primes of form $4k+1$. Denote these primes as $p_1, p_2, \dots, p_n$. Define

$$\begin{aligned} N :&= (2p_1p_2 \dots p_n)^2 + 1 \\ &\equiv 4 + 1 = 1 \pmod 4 \end{aligned}$$

By FTA, $N = q_1q_2 \dots q_n$ where each q_i's must be of form $4k+3$ since they are odd and not of form $4k+1$ which doesn't divide N. Let $q = q_1$, a prime factor of N of form $4k + 3$. Hence

$$(2p_1p_2 \dots p_n)^2 + 1 \equiv 0 \pmod q \implies (2p_1p_2 \dots p_n)^2 \equiv -1 \pmod q.$$

This can happen if and only if $q \equiv 1 \pmod 4$ [by WS5 P4, to be shown on Wed]. (Because squares can only be 0 or 1 mod 4 and so q can only be $0 + 1$ or $1 + 1$ mod 4. Since q is odd, it cannot be $1 + 1$ mod 4 and can only be $0 + 1$ mod 4. This shows that q has to be of form $4k + 1$.) □

Problem 1

Show that there are infinitely many primes that are 1 mod 3.

Solution

Assume, for contradiction, that there were only finitely many primes of form $3k+1$. Denote them as $p_1, \dots, p_n$. Define

$$N := (2p_1p_2 \dots p_n)^2 + 3$$

Again, pick $q = q_1$ and we have

$$(2p_1p_2 \dots p_n)^2 \equiv -3 \pmod{q}.$$

Since $q \neq 2, 3$, it must be of form $3k+1$ since squares can only be 0 or 1 mod 3, and squares +3 can only be of form $3k$ or $3k+1$.

Remark

When dealing with special cases of Dirichlet's Theorem, always first check the possible modulo results of a square. Then sometimes we can derive a contradiction.

8 Fri 10/15