# Notes

May 7, 2014

## 9/26

Number theory is(?) the properties of numbers (integers) and variations and relations to other numbers. Common Symbols:

- $\mathbb{Z}$: Integers
- $\mathbb{Z}[i]$: Gaussian integers, which is the set of $\{a + ib | a, b \in \mathbb{Z}\}$.
- $\mathbb{R}$: Real Numbers
- $\mathbb{Q}$: Rational Numbers

Some types, in fact, sequences of "numbers" (usually integers or positive integers)

1. squares: $0, 1, 4, 9, 16, \ldots$
2. primes: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$
3. Fibonacci: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

$\exists$ infinietely many primes? "Yes" (provable)
$\exists$ infinitely many Fionacci primes? "Yes" (open problem)
Is every positive integer/big enough positive integer a sum of $\leq$ 2, 3, 4, 17 primes? squares? Fibonacci numbers?
Every $n > 0$ a sum of two squares? NO, 6. (proved outright)
$(\exists C)$ Every $n > C$ a sum of two squares? No (provable?)
For 3 squares, No
What about a sum of four squares? Yes, sort of deep Theorem
Given $k > 2$, Every $n > 0$ is a sum of $k$ Fibbonacci numbers? k=2, no (12). Eh... any k, no by another proof.

Theorem: $(\forall k)(\exists n > 0)(n$ is not a sum of $k$ Fibbonacci numbers).

## 9/29

### Questions

Are there infinitely many? Are all sufficiently large, or all number of sum of __ many of some type?
Betweeness: Are there any primes between two Fibonacci numbers (after a few )? Are there primes between two squares? Yes (proven) and Yes?(eh... still a conjecture.)
Irrationality, approximation. We know that $\sqrt{2}$. What about $2^e$?
Is $\sqrt{2} \approx \frac{a}{b}$ where $a, b$ are integers.

### Proofs

One method is induction. You can assume all previous cases provided there is always a earlier remaining case. Induction principle: Every non-empty subset of $\mathbb{Z}$ has a least element.
Induction does not work for $\mathbb{R}_{\geq 0}$. Why? We have a first case, but once you assume a case, you cannot move over to the next set because what is the next set?

**Proof by Induction**

Theorem: In a game of football with touchdowns and field goals with 3, 6, and 7 points, every score of at least 12 points is reachable.
We can get 12 points from 6+6.
We can get 13 points from 6+7.
We can get 14 points from 7+7.
Let's assume that we did case n - 3. How do we attain n? Do n - 3 and attain a 3 point, you get n.
That's our proof. We did the earliest possible 3 cases and used induction to attain the next 3.

**Proof by Contradiction**

Theorem: $\sqrt{2} \neq \frac{a}{b}$.
Proof: Let's assume the first counterexample. The first counterexample is the first $b$. We'll asume that $\sqrt{2} = \frac{a}{b}$. Then, $a^2 = 2b^2$. That means that a is even. Let $a = 2c$. Then, $4c^2 = 2b^2$. Then, $b^2 = 2c^2$. Since $c < b$, $\frac{b}{c}$ is an earlier counterexample than $\frac{a}{b}$, a contradiction. You claim that $\frac{a}{b}$ is the earliest counterexample, but now we see that it is not the earliest counterexample. There was an earlier. That means that there is no counterexample.

**Method of Congruences**

Means divide numbers by some a, look at remainders.
E.g. $n = 4k + 1$ is a congruence mod 4 or $n = 10k + 3$, numbers with last digit 3.

Theorem: $\exists$ arbitrary large $n$ which are not the sum of two squares.
100,003 e.g. or any $n = 4k + 3$.
Proof Say $n = 4k + 3$.

$$\begin{aligned} (4a)^2 &= 16^2 \\ (4a+1)^2 &= 16a^2 + 8a + 1 \\ (4a+2)^2 &= 16a^2 + 16a + 4 \\ (4a+3)^2 &= 16a^s + 24a + 9 \end{aligned}$$

mod 4 of the above four is 0, 1, 0, 1 respectively. That means all squares are 0 or 1 mod 4. So, $a^2 + b^2$ is 0, 1, or 2 mod 4. It is never 3. Therefore, there exists arbitrary large $n$ which are not the sume of two squares.

Theorem: There exists arbitrary large n which are not the sum of 2 Fibonacci number.
Proof: (By Counting)
Example: $f_n < 200$: 0, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 134. Only 12 of them. If $n \leq 200, n = f_a + f_b$ using 12 numbers. You can only get at most $12 * 12 = 144$ choices for 200 numbers. That is impossible. Let's generalize this tomorrow.

Let $a(C)$ be the number of Fibonacci numbers. $(\exists k > 0)a(C) \leq k(\ln C)$ for $C \geq 10$. Then, we wanted $n = f_\alpha + f_\beta$.
Number of choices for $n$: $C + 1$. for $f_\alpha$, $a(C)$, for $f_\beta$, $a(C)$.
Number of choices on the right hand side: $a(C)^2$ and that's less than or equal to $k^2(\ln C)^2$.
Number of choices on the left hand side: $C + 1$
We know that $\lim_{C\to\infty} \frac{k^2 \ln C^2}{C} = 0$. Therefore, the number of numbers formed by the sum of the fibonacci numbers is less than there is numbers.

# 10/1

$a|b$. $a$ is the dividend and $b$ is the divisor.
Will often be written as $a = bq + r$ where $r$ is the remainder, which is of the set of integers starting with 0 to $|b| - 1$. $q$ and $r$ are unique.
Ex) Let $a = -4$ and $b = -3$. The quotient is 2 with remainder 2.

Ex) if $b = 4$, then $4q, 4q + 1, 4q + 2, 4q + 3$ are all four possibilities of all numbers listed once each.
Ex) if $b = 2$, then $2q, 2q + 1$ are the only two possibilites, which are even and odd, respectively.

## Prime Numbers

Several deep facts, which are very familiar:

1. $\exists$ infinitely many prime numbers
2. Every number greater than 1 has a prime factorization.
3. It's unique up to order.

### Proof of Fact 2

Proof by double induction (or perform induction twice)
Lemma: Given $n > 1$, $n$ has a prime factor, $p$.
$n$ has a smallest factor, $a$, or $a|n$ where $a > 1$.
If $a$ weren't prime, it would have a factor(divisor), $b > 1$ where $b|a|n \implies b|n$. That is a contradiction since $a$ was supposed to be a smallest factor of $n$, but $b$ is also a factor and is smaller than $a$.
Main proof: By direct induction, say $n > 1$ is the first remaining case. $n$ has a prime factor, $p$, by the Lemma.
From here, $n = p$ or there exists another integer, $q$, such that $n = pq$. $q$ has a prime factorization by the Lemma. $\square$

### Proof of Fact 1

There are infinitely many primes.
Proof: Supposed that there are only finitely many primes say $k$. Let $n = p_1 \dots p_k + 1$ where $p_i$ is a the $i$th prime number. $n > 1$ since 2 is one of the primes. $n$ is divisible by some prime, which cannot be $p_1, p_2, \dots, p_k$, but those were supposed to be all the primes. There cannot be another! We have a contradiction.

### Variation of Fact 1: primes and congruences

Even has only one prime: 2
Odd has infinitely many.

mod 3

1. 3k - finitely many primes, 1 in fact, 3.
2. 3k + 1 - infinitely many primes? 7, 13, ...
3. 3k + 2 - infinitely many primes? 5, 8, 11, 17, ...

We know at least $3k+1$ and/or $3k+2$ has to contain infinitely many primes since $3k, 3k+1, 3k+2$ cover the entire space of non-negative real numbers.

Theorem: $\exists$ infinitely many primes of the form $3k+2$. Lemma: $(1 \mod 3)(1 \mod 3) = (1 \mod 3)$ Why? $(3b+1)(3a+1) = 9ab + 3(a+b) + 1 = 3(3ab + a + b) + 1$
Say that there are finite number of primes, $p_1, \dots, p_k$ that are $2 \mod 3$. Then, let $n = 3p_1p_2 \dots p_k + 2$. $n$ has a prime factorization. $s \not| n$ Proofs are all either $1 \mod 3$ or $2 \mod 3$. Not all of them are $1 \mod 3$ because then, n would be.
So, there exists $p$, $p = 3k + 2$ suc that $p|n$. CONTRADICTION! Therefore, there are infinitely many of them.

# 10/3

## Prime Proof continues

Lemma 1: $(1 \mod 3)(1 \mod 3) = 1 \mod 3$.
Lemma 2: If $n \equiv 2 \mod 3$, so its at least one of its prime factors.
Proof: See Lemma 1. $3 \not| n$, all prime factors are 1 or $2 \mod 3$. Can't all be $1 \mod 3$.
Main Proof: Suppose $p_1, \dots, p_k$ were all of the prime numbers. Let $n = 3p_1 \dots p_k - 1$.
Is $n > 1$? yes
Is $n \equiv 2 \mod 3$? Yes
So, by Lemma 2, some prime factors of $n$ is $2 \mod 3$ and it isn't $p_1, p_2, \dots, p_k$! Contradiction.

Ex) Suppose you thought $2, 5, 11$ was all.
Then, $n = 3 * 2 * 5 * 11 - 1 = 330 - 1 = 329 = 4 * 47$. 329 isn't prime, but 47 is.

Non-Proof: $n = 3p_1p_2 \dots p_k + 2$ instead. This doesn't imply a new prime factor, which is 2 mod 3.
Ex) Say $2, 5$ is all you have. $n = 3 * 2 * 5 + 2 = 32 = 2^5$, which is not a prime.

Unique factorization is a harder theorem to prove. The proof depends on greatest common factors (gcd).

### Big Oh notation

$O(f(n))$ means any function less than $C * f(n)$.

Ex) Adding two n-digit numbers. $O(n)$. Usually $C * n$ work, but can't be slower. Could be faster.
Ex) Multiplying two n-digit numbers in elementary school way. $O(n^2)$
Worrying about some number $N$ with $n$ digits. $N = O(10^n)$ with $n = O(\log(N))$.
Usual primality/factoring method trial divisions.
$2|N$, $3|N$, ..., $\lfloor\sqrt{N}\rfloor|N$.
Amazing Theorem: There exists approximately $\frac{N}{\log(N)}$ primes up to $N$.

1 trial division is $O(n^2) = O(\log(N^2))$ work.
Total work: $O(\sqrt{N}\log(N)) = O(10^{\frac{n}{2}})$
Truth: Primality is (we think) much eaiser than factoring.
Primality has a $O(n\log(n))$ probabilistic method.

### GCDs

Two definitions:

1. Literal: Here also gcd(a,b) = (a, b) means largest d such that $d|a, b$

2. Share - gcd, d = /pi o

Ex) gcd(24, 60) = $gcd(2^3 * 3, 2^2 * 3 * 5)$.

## 10/6

### More about proofs

We did infinitely many primes of $3k + 2$. In book, Rosen does primes of $4k + 3$. He creates the number, $n$, such that $n = 4p_1 \dots p_k + 3$. We don't want $p = 3$. Book leaves out $p_0 = 3$. It still works out. Different ways to prove something.

### Algorithms and bases

Have some computation with $N$ and $N$ has $d$ digits, then $N = O(10^d)$. and $d = O(log_bN)$. We know that $10^{b-1} \leq N \leq 10^b - 1$.
$O(f(n))$ is actually just $\leq Cf(n)$.
$O(10^d)$ means that $N \leq C10^d$. 2-sided version of $\Theta(f(n))$.
$N = \Theta(10^d)$ is true too since the best case is also that.
But, the computer's actual work is not usually in base 10. It's in base 2. Arithmetic algorithms of base 10 works in other bases.
Adding/Subtracting takes $O(d_8)$ work in base 8 and $O(d_10)$ work in base 10. They're both the same since the number of digits in base a is almost the same as number of digits in base 10.
$O(\log_a N)$ vs. $O(\log_b N)$
$\log_a N = (\log_b a)(\log_b N)$ and $\log_b a$ is constant.

Ex) $173_8 = 3k + 3$
Generalization: Last j digits are remainder had $b^j$.
Ex) $7546282 = 1000k + 282$
$173_8 = 64k + 73_5 = 64k + 59$.

### Ways to define GCD

1. Literal gcd: $d = (a, b) = gcd(a, b)$ is the biggest integer that divides both. (Exists and is unique, but short on properties)
2. share gcd: $d =$ product of primes shared by both in a factorization (exists, but not unique without unique factorization)
3. strong gcd: $d$ is a number, $d = xa + yb$, where $x$ and $y$ are integers. In general, $x$ and $y$ can be negative.

Ex) gcd of 10 and 6? $d = 2$ is the literal gcd. Is it a strong gcd? $2 = 10x + 6y$. Well... $x = 2$ and $y = -3$. Yes!
What makes it "strong"?
First of all, a strong gcd is a literal gcd. Say, $d = ax + by$ and $d|a, b$. Say $e|a, b$, then $e|xa + by$ for all $x, y$, so in particular $e|a$. $d$ is not just $\geq$ any common divisor, e, it's a multiple, $e|d$.
Any share gcd is a common divisor. $d$ is a multiple of it and our strong gcd is a shared gcd.

Theorem: (proof by algorithm) Every $a, b$ have a strong gcd and all three versions are the same.

## 10/8

### GCD continued

Theorem: strong gcd = shared gcd Proof: (share gcd = strong gcd) In other words, $xa + yb = d$ and $d|a, b$.
Divide the former by $d$. We get $x\frac{a}{d} + y\frac{b}{d} = 1$
So, $\frac{a}{b}, \frac{b}{d}$ share no factor. So, $a =$ (factorization of d)(factorization of $\frac{a}{d}$) and $b =$ (same factor of of d) (factor of $\frac{b}{d}$). These factors make d a shared gcd.

Proof of theorem from previous class: Let's do induction on $a + b$.
Have $a, b$ done for all previous cases. Without loss of generality, $a > b$ (because otherwise, switch them). Now, let's look at the division algorithm.
Theorem: $a = qb + r$.
By induction, $b + r$ have strong gcd, $d$, unless $r = 0$.
Let's have an emergency side case: $r = 0$. Then, $a$ is a multiple of $b$ making $b$ the strong gcd.
Otherwise, $r > 0$. Then, $d = xb + yr$ and $d|r, b \to d|a$, and $d = xb + y(a - qb) = ya + (x - yq)b$.
The algorithm form. Keep two numbers. Keep dividing one into the other to make a remainder. Keep doing that until integral combination of original $a, b$.

Ex) gcd of 42 and 16. Euclidean Algortihm

| | | |
|---|---|---|
| 42 | 1 | 0 |
| 16 | 0 | 1 |
| 10 = 42 - 2*16 | 1 | -2 |
| 6 = 16 - 10 | -1 | 3 |
| 4 = 10 -6 | 2 | -5 |
| 2 = 6 - 4 | -3 | 8 |

Fact: After 2 steps into the Euclidean algorithm has return in half. Then, it's $O(loga)$ steps or $O(n)$ if $a$ has $n$ digits $(a \geq b)$.
$O(n)$ rounds times $O(n^2)$ work for division $= O(n^3)$ total work.
Actually, total work is only $O(n^3)$.

### Unique Factorization Theorem

Primality Lemma: If $p$ is prime and $p|ab$, then $p|a$, $p|b$, or both.
Proof: Suppose to the contrary that $p \not| a$ and $p \not| b$.
Since $p$ is prime, then the only divisor is $1, p$.
Then, $gcd(a, p) = 1$ and $gcd(b, p) = 1$.
Then, by the strong gcd theorem, $x_1a + y_1p = 1$ and $x_2b + y_2p = 1$.
How about multiplying them with each other.

Creative step:

$$\begin{aligned}(x_1a + y_1p)(x_2b + y_2p) &= 1\\ x_1x_2ab + p(x_2y_1b + x_1y_2 + x_2y_1p) &= 1\end{aligned}$$

But, p divides ab, so how does that result in their gcd being 1? Contradiction!

# 10/10

## Unique Factorization continued

Primality Lemma: If $p$ is prime and $p|ab$, then $p|a$ or $p|b$.
Theorem: All factors of $n > 1$ are the same up to order.
Proof: Say $n = p_1 \dots p_k$ and $n = q_1 \dots q_l$ where $p_i, q_i \in \{$ primes $\}$ and both sets are not identical.
We can suppose that by induction that the two factorizations are disjoint. If there are elements in both factorization, then, we can remove them from both factorizations with a smaller number with two factorization with disjoint set of primes.
So, what we have are:
$n = p_1p_2 \dots p_k$ and $n = q_1q_2 \dots q_l$ with $p_a \neq q_b$
Since $p_1$ divides $n$, so $p_1$ divides $q_1q_2 \dots q_l$.
Then, $p_1|q_b$ for some b.
Then, $q_b$ is either not prime or equal to $p_1$, but both are impossible by our assumption. CONTRADICTION!

(Former)If $p = ab$, then $p|a$ or $p|b$.
(Latter)The lemma is if $p|ab$, then $p|a$ or $p|b$, which is stronger.
In more general number system,

1. The former definition is called "irreducible"
2. The latter definition is called "prime"

Lemma: "irreducible" $\Rightarrow$ "prime"

"Application" of the unique factorization.
Theorem: $\sqrt{n}$ is irrational unless there exists an $c$ such that $n = c^2$.
Proof: Say that $n = \frac{a^2}{b^2}$, then $a^2 = b^2n$. Let $k = a^2$. $a^2$ has a unique factorization. The unique factorization of $k =$ factorization of a twice = (factorization of $n$) * (factorization of $b$ twice).
That means that all of the factors of $n$ must appear an even number of times. In other words, it's a square of something.
Informally, $\sqrt{60} = \sqrt{2 * 3 * 5}$ is irrational because you cannot divide $2, 3, 5$ by 2 and get an integer.

## Congruences

Defintion: $a \equiv b \mod n$ means that $n|a - b$. It reads as "$a$ is a congruence of $b$ mod n."
Example: $7 \equiv 79 \mod 9$
$a \equiv b \mod 2$ - same parity
$a \equiv b \mod 10$ - some unit digit.
This is only reasonable if

1. $a \equiv a$ (Identity)
2. $a \equiv b \Rightarrow b \equiv c$ (Symmetry)
3. $a \equiv b$ and $b \equiv c \Rightarrow a \equiv b$ (Transitivity)

If $n|a - b$ and $n|b - c$, then $n|a - c = (a - b) + (b - c)$ because of primality lemma.

# 10/13

$a \equiv b \mod n$ means $n|a - b$
It's an equivalence relation. We got a partition of $\mathbb{Z}$ into equivalence classes called congruence classes.
$\bar{a}$ is the congruence class of $a$. $\bar{a} = \bar{b}(\mod n)$ or $\bar{a} = \bar{b}$ means that that $a \equiv b \mod n$ or $\bar{a} = \bar{b}$ means that that $a \equiv b$

mod $n$
Example: mod 2
$\bar{1}$ is the equivalence class of 1 mod 2 = set of odd numbers
For example, $\{-3, -17, 1, 27, \ldots\}$
$\bar{0}$ is the equivalence class of 0 mod 2 = set of even numbers
For example, $\{-2, 0, -20, 4\}$

A lot of synonyms:
$\bar{1} = \bar{3} = \bar{17}$( mod 2) or in congruence from $1 \equiv 3 \equiv 17 \equiv \ldots$ ( mod 2)
It is also good to have standard name.
Let $a = qn + r$.
$n$ is our modulus. $r \in \mathbb{Z}$ and $r \in [0, n-1]$. Any set of standard names are called residues. $0, 1, \ldots, n-1$ are "least positive residues"
Example: mod 12
$0, 1, \ldots, 11$ is a standard
$1, 2, \ldots, 12$ is another standard. $0 \equiv n$ mod $n$.

Centered standard is also important. $n = 2k + 1$, use $-k, -k+1, -k+2, \ldots, k$
Example: mod 7
$-3, -2, -1, 0, 1, 2, 3$ is the complete set of residues.

Example: Odd numbers are numbers of the form $4k \pm 1$, just as they are $4k + 1$, $4k + 3$.

Theorem: Congruences is compatible with $+, -$, and $*$.
Note: NOT DIVISION!
If $a \equiv b$ mod $n$, then $a + c \equiv b + c$ mod $n$. (can then replace both $a$ and $c$.)
The same can be said about subtraction.
If $a \equiv b$ mod $n$, then $ac \equiv bc$ mod $n$.
Proof: Say that $a = qn + b$. Then, $a + c = qn + b + c$. We say that $a + c \equiv b + c$.
Same with subtraction.
Multiplication version. $ac = (qn+b)c = cqn+bc$, which means that $ac \equiv bc$ mod $n$. Say that $a = q_1n+b$ and $c = q_2n+d$.
I want $ac \equiv bd$ mod $n$. Slick version use the theorem twice.
Direct version:

$$\begin{aligned} ac &= (q_1n + b)(q_2n + d) \\ &= (q_1q_2n^2 + dq_1n + bq_2n + bd) \\ &= n(\text{stuff}) + bd \end{aligned}$$

Example: $3k_1 + 1$ times $3k_2 + 1$ is $3k_3 + 1$.
New phrasing is that $1 * 1 \equiv 1$ mod 3.
Example: $7k_1 + 4$ times $7k_2 + 5$ is $7k_3 + 6$ because $4 * 5 = 20 \equiv 6$ mod 7.
Example: $769k_1 + 769$ times $769k_2 + 765$ is $769k_3 + 1$.
New form: $768 * 768 \equiv -1 * -1 \equiv 1$ mod 769. Negative makes things easier.

Definition$\mathbb{Z}/n$ is the set of congruence classes. The bars indicate a set.
Example: $\mathbb{Z}/2 = \{\bar{0}, \bar{1}\}$
$\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{-1}, \bar{-2}, \bar{-3}\}$

Complete arithmetic tables for $\mathbb{Z}/2$:

| $+$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| $*$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ |

Complete arithmetic tables for $\mathbb{Z}/4$:

| $*$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{1}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

# 10/15

One notion of negative that works
$-(\bar{a}) = \bar{-a}$
Meaning that subtraction works.
Another description: $\forall \bar{a} \exists \bar{b}$ such that $\bar{a} + \bar{b} = \bar{0}$.

Is Division closed in the same sense? In other words, is this true? $\forall \bar{a} \exists \bar{b} such that \bar{a}\bar{b} = 1$.
Let's think of reciprocals first.
Some problems:
By the tables above, $\bar{1}/\bar{0} = \bar{0}$, but we can't divide 0.
What about $\bar{2}/\bar{2}$? Is it $\bar{1}$ or $\bar{3}$?

$\bar{2} = \{2, 6, 10, 14, \ldots\}$. It's an abstract form of the point that divisions is tricky.

Ex) mod 10
$a \equiv 1 \mod 10$
$b \equiv 7 \mod 10$
You can try $\frac{1}{7} \mod 10$, but what is $\frac{1}{7}$? It's not integer. Really, what you are doing is the following:
$\frac{a}{b} = \frac{\ldots 1}{\ldots 7} = \ldots 3$ ALWAYS! when $b|a$
So, we say that that $\frac{1}{7} \equiv 3 \mod 10$.

Other examples for mod 10
$\frac{\ldots 1}{\ldots 5} \equiv DNE \in \mathbb{Z}$, so $\frac{1}{5} \equiv DNE \mod 10$. DOES NOT EXISTS!!!!
$\frac{\ldots 5}{\ldots 5} = \begin{cases} \ldots 1 \\ \ldots 3 \\ \ldots 5 \\ \ldots 7 \\ \ldots 9 \end{cases}$. This is also considered "Does not exists".
Book's description of something.
Solve: Let $7x \equiv 1 \mod 10$ means that $x \equiv 3 \mod 10$
$5x \equiv 1 \mod 10$ means no solution
$5x \equiv 5 \mod 10$ means that $x \equiv 1, 3, 5, 7, 9$

Definition: $a$ and $b$ are relatively prime means $gcd(a, b) = 1$ or $a \perp b$.
$a_1, \ldots a_n$ are relatively prime if $a_j \perp a_k$ for $\forall j, k$ where $j \neq k$.
Examine the equation: $ax \equiv 1 \mod n$.
Then, $n|ax - 1$ or $\exists y$ such that $ax - 1 = yn \Rightarrow ax - ny = 1$.
$xa - yn = 1$ iff $gcd(a, n) = 1$.
That's exactly whn $\frac{1}{a}$ exists, has at least one solution.
The set of these a's are the prime residues where mod n occurs.
$ax \equiv 1 \mod n$ has at least one solution, $x$, but $\frac{1}{a} \mod n$ is only reasonable if there exists at least one solution.
Fact/Theorem: $ax \equiv b \mod n$ if $\exists$ exactly one solution. If $(a, n) = 1$, has exactly one solution $x \mod n$ for all b.
Proof: $ax \equiv 1 \mod n$ has $\geq 1$ solution, did this already.
So, $ax - b \mod n$ has $\geq 1$ solutions, multiply b.
By the piegonhole principle,
General case of $ax \equiv b \mod n$
$gcd(a, b) = d$.
No solutions unless $d|b$ because otherwise, $d|n$, but $d \not| ax - b$. If $d|b$, there are $d$ solutions.

# 10/20

## More mod fun

Given $a$ and mod $n$, $\frac{1}{a}$ exists mod $n$ or $\frac{1}{a} \in \mathbb{Z}/n$ when $gcd(a, n) = 1$.
mod $n$ is a ring.
Ex) $\frac{1}{2} \equiv x \mod 7$. $x$ is 4 because $4 * 2 = 8$ which is 1 mod 7.
Ex) $\frac{1}{8191} \equiv x \mod 1,111,111$. Takes way to long to factor, so solve $5191x + 1,111,111y = 1$ by Euclidean Algorithm.
Exponentiation of mod $n$

Two tricks:

1. You can reduce $\mod n$ in the middle without changing the center.

In the former case, Ex) $2^7 \mod 9$.
Silly way: plow through!
Better way: 2, 4, 8, 7($16 \equiv 9$), 5, 1, 2, 4, 8, 7, 5.
We get that 2 is the answer.
Another way: Square up! The silly way, but more efficient. $2^16 \equiv 4^8 \equiv 8^4 \ldots$. What about odd exponents? $2^17 \mod 13$.
Well... just add exponents to string up $2^17$ like... $2^17 = 2^16 * 2$.
So, $a^b \mod n$ is fast. How fast? $O(d^2)$ work for each multiplication. $O(\log_2 b)$ multiplies because it is $O$(number of digits of b). We get $O(d^3)$ since $d$ is the max digits in $a, b, n$.
What about $a^{-b}$? Well... $a^{-b} = (a^{-1})^b$, so it's fast too.
One more reciprocol trick.
Ex) $10! \mod 11$.
$1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10$
continue next time

# 10/22

If a set has $+, -, *$ (with suitable axioms that I'm skipping), it's a ring.
If a set has $+, -, *, /$ (except for $\frac{a}{0}$) with suitable axioms, it's a field (and a ring).
Ex) $\mathbb{Z}$ is a ring, $\mathbb{N}$ is semi-ring, and $\mathbb{Q}$ is a field.
We can perform linear algebra in any field!
Also, many field can solve the following: 1) $ax = b$ if $a \neq 0$ since you can do $x = \frac{b}{a}$.
2) It can solve systems of equations.
If we wanted $\mathbb{Z}/n$ to be a field, we would want any residue, $a$, to have $\frac{1}{a}$, i.e. $gcd(n, a) = 1$.
Theorem?: Unless $a \equiv 0 \mod n$, we want $gcd(a, n) \equiv 1$ unless $n|a$. This is true $\forall a$ exactly when $n$ is prime.
Theorem: $\mathbb{Z}/n$ is a field iff $n$ is prime.
Theorem: $\mathbb{Z}/p$ is a field and $\mathbb{Z}/ab$ isn't.
Ex) For $\mathbb{R}/3$: $\frac{1}{1} \equiv 1$, $\frac{1}{2} \equiv 2$.
For $\mathbb{R}/13$: $\frac{1}{1} \equiv 1$, $\frac{1}{2} \equiv 7$, $\frac{1}{3} \equiv 9$, $\frac{1}{4} \equiv 10$, $\frac{1}{5} \equiv 8$, $\frac{1}{6} \equiv 11$, $\frac{1}{-6} \equiv -11 \equiv 2$, $\frac{1}{-5} \equiv -8 \equiv 5$, etc...
For $\mathbb{Z}/(13(17)$, $\frac{1}{13}$ does not exist because $13x \not\equiv 1 \mod 13 * 17$ is not field

Wilson's theorem: If $p$ is prime, then $(p-1)! \equiv -1 \mod p$ or $p|(p+1)! + 1$.
Ex) 61 is prime. Now, by Wilson's Theorem, $60! + 1$ is divisible by $(p-1)!$. It is not divisible by all primes $< 60$ because 60! is a multiple of all primes under 60. Adding 1 will prevent it.
Proof: Idea is to marry residues in pairs. $a$ marries $b$ when $ab \equiv 1$, so $a \equiv \frac{1}{b}$.
This is only reasonable if $a \neq b$. What's left is $a \equiv \frac{1}{a}$ or $a^2 \equiv 1 \mod p$.
Certainly, $a \equiv 1$, $a \equiv -1$ remain. Anything else? No
As $a^2 - 1 \equiv 0 \mod p$. We want to show $a \equiv 1 \mod p$.
Then, $p|a^2 - 1 \equiv (a+1)(a-1)$, so $p|a+1$ or $p|a-1$ by the old primality lemma.
So, to conclude, all factors of $(p-1)!$ cancel mod p except $1, -1$, so get $(p-1)! \equiv -1 \mod p$ assuming $1 \not\equiv -1$. This is ok if $p \neq 2$.
If $p$ is 2!, this is a special case. $1! \equiv 1 \mod 2$.

$(\mathbb{Z}/n)^x$ = set of prime residues doesn't have + or −, but has $*$, if $\frac{1}{a}, \frac{1}{b}$ exists, so does $\frac{1}{ab}$.
It has also has division. $\frac{b}{a} \equiv b\frac{1}{a}$.
This is known as a group.
Note: prime residues mean that all the residues are coprime.

# 10/24

## A loose end

Solving $ax \equiv b \mod n$ when $\frac{1}{a}$ does not exists.
Two possibilities:

1. gcd(a,b) = d ¿ 1, then multiple solutions

2. If $d \not| b$, no solutions.

$d(\frac{a}{d}x) \equiv d(\frac{b}{d}) \mod n$.
What does multiplying by $d|n$ do?
$x \mod n$ determines $x \mod \frac{n}{d}$ and then $dx \mod n$ is $d$ times that.
So, $dx \equiv dy \mod n$
iff $x \equiv y \mod \frac{n}{a}$
so, $d(\frac{a}{d}x) \equiv d(\frac{b}{a}) \mod n$ becomes $(\frac{a}{d}x \equiv \frac{b}{a} \mod \frac{n}{d}$, $gcd(\frac{a}{d}, \frac{n}{d}) = 1$.
So, now multiplier, $c = \frac{a}{d}$ has a reciprocal.
$\frac{1}{c} \mod \frac{b}{d}$

Ex) $30x \equiv 70 \mod 290$
Rewrite: $3x \equiv 7 \mod 29$
1 solution is $\mod \frac{n}{d}$, which is 29 in this case. $d$ solutions $\mod n$. (10 solutions for $\mod 290$).

$x \mod a$ determines $x \mod b$ when $b|a$ and not otherwise.
One determines many as some question.
From $x \mod 60$ can you get $x \mod 15$ and $x \mod 4$ and $x \mod 6$
Ex) Two small congruences ⇒ one big one.
I have $x \mod 12$, can I get $\mod 3$ and $\mod 4$.

| mod 12 | mod 3 | mod 4 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 2 | 2 | 2 |
| 3 | 0 | 3 |
| 4 | 1 | 0 |
| 5 | 2 | 1 |
| 6 | 0 | 2 |
| 7 | 1 | 3 |
| 8 | 2 | 0 |
| 9 | 0 | 1 |
| 10 | 1 | 2 |
| 11 | 2 | 3 |

$3|x$ and $4|x \Rightarrow 12|x$ because $lcm(3,4)|x$ and $lcm(3,4) = 12$.

LCM's are a lot like gcd's especially since shared gcd defintion.
$a$ and $b$ have prime factors. Each is a "bag" of primes. Actually, multiset, a set of repeats.
Ex) $8 = 2 * 2 * 2$
$12 = 2 * 2 * 3$
$gcd(8, 12) = 2 * 2 = 4$
Shared LCM is $\uplus$. In this case, $2 * 2 * 2 * 3$.
$lcm(8, 12) = 24$.
Theorem: $lcm(a, b) = \frac{ab}{gcd(a,b)}$.
All we needed in $\mod 3$, $\mod 4 \Rightarrow \mod 12$.

small Chinese Remainder Theorem: If $gcd(a, b) = 1$, then $x \mod a$ and $x \mod b$ determine $x \mod ab$. In fact, you get a bijection between the $ab$ values on both sides.
Proof: Since $gcd(a, b) = 1$, we know $lcm(a, b) = ab$.
So, therefore, if $x \equiv 0 \mod a$ and $\mod b$. It is $\equiv 0 \mod lcm(a, b) = ab$.
So, if $x \equiv y \mod a$ and $x \equiv y \mod b$.
$x - y \equiv 0 \mod a$ and $\mod b$ or $x - y \equiv 0 \mod ab$ or $x \equiv \mod ab$, which is what we wanted.
There is a function $f$ from $\mathbb{Z}/ab$ to $(\mathbb{Z}/a)X(\mathbb{Z}/a)$. We showed $f$ is injective. They are also surjective.
Theorem: If $gcd(a_i, \ldots, a_j) = 1$, where $a_i \perp a_j$, then there's a bijection $(\mathbb{Z}/a_1)X(\mathbb{Z}/a_2)X \ldots X(\mathbb{Z}/a_j) \Leftrightarrow (\mathbb{Z}/a_1a_2 \ldots a_k)$.

# 10/27

## Chinese remainder theorem

Little theorem: If $gcd(a, b) = 1$ and $a \perp b$, then the reductions from $\mathbb{Z}/ab$ to $\mathbb{Z}/a$ and $\mathbb{Z}/b$ yield a bijection: $\mathbb{Z}/ab \to \mathbb{Z}/a$ X $\mathbb{Z}/b$.

What to call an element of $\mathbb{Z}/a$ X $\mathbb{Z}/b$?
Usually $(\bar{x}, \bar{y}) \in \mathbb{Z}/a$ X $\mathbb{Z}/b$, but we use this for gcd. Please use gcd in front of $(x, y)$ because it's confusing otherwise.

The real(or big) Chinese remainder theorem: If $a_1, \ldots, a_k$ are all coprime and $n = a_1 a_2 \ldots a_k$, then reduction gives you a bijection: $\mathbb{Z}/n \leftrightarrow \mathbb{Z}/a_1$ X $\mathbb{Z}/a_2$ X ... X $\mathbb{Z}/a_k$
Proof: By Induction on $k$.
If $k = 2$, then just little Chinese remainder theorem will work.
If $k > 2$, let $m = a_1 a_2 \ldots a_{k-1}$.
Little Chinese Remainder theorem gives us that $\mathbb{Z}/n \leftrightarrow \mathbb{Z}/m$ X $\mathbb{Z}/m_k$
Induction gives us $\mathbb{Z}/m \leftrightarrow \mathbb{Z}/a_1$ X ... X $\mathbb{Z}/a_{k-1}$. Combine them.

Ex) 60 = 4 * 3 * 5

$$\begin{aligned} \mathbb{Z}/60 &\leftrightarrow \mathbb{Z}/4 \text{ X } \mathbb{Z}/15 \\ &\leftrightarrow \mathbb{Z}/4 \text{ X } \mathbb{Z}/3 \text{ X } \mathbb{Z}/3 \end{aligned}$$

The second equation is as a result of $\mathbb{Z}/15 \leftrightarrow \mathbb{Z}/3$ X $\mathbb{Z}/5$.

The constructive Chinese Remainder Theorem: $\mathbb{Z}/ab \to \mathbb{Z}/a$ X $\mathbb{Z}/b$.
Ex) $\mathbb{Z}/2047 \to \mathbb{Z}/23$ X $\mathbb{Z}/89$
$\not\vdash\not\vdash\not\vdash \to (\not\leftarrow, \not\vdash\not\vdash)$
Going backwards is harder, but there is an algorithm for it.

Building an explicit inverse given, 2nd proof needed.
The plan is to first compute CRT basis on $\mathbb{Z}/ab$.
Let $\bar{x} \to (\bar{1}, \bar{0})$ and $\bar{y} \to (\bar{0}, \bar{1})$
Then, $\bar{x} + \bar{y} \to (\bar{1}, \bar{2})$
We want $x \equiv 1 \mod a$ and $x \equiv 0 \mod b$, so $x = sb$ and $x + ta = 1$. Then, $sb + ta = 1$.
Then, $x = sb$ is the basis to the solution of $(\bar{1}, \bar{0})$.
$y = ta = 1 - x$ is the other one.

Ex) Extended European Algorithm (EEA) for 23 and 89

| | | | |
|---|---|---|---|
| 89 | 23 | a = 23, b = 89 | |
| 20 | 23 | 20 = b - 3a | |
| 20 | 3 | 3 = a - (b - 3a) = 4a - b | So, $x = -8*89 \equiv$ |
| 2 | 3 | 2 = b - 3a - 6(4a - b) = 7b - 27a | |
| 2 | 1 | 1 = 4a - b - (7b - 27a) = 31a - 8b | |

$1 \mod 23 \equiv 0 \mod 89$
$y \equiv 31 * 23 \equiv 0 \mod 23 \equiv 1 \mod 89$.
so, $x + 2y \equiv 1 \mod 23 \equiv 2 \mod 89$.

### $\cong$: Isomorphism

Ex) $\{one, two\} \neq \{un, deux\}$. The latter is French for one and two.
However, $\{one, two\} \cong \{un, deux\}$. The reason is because it preserves properties like un + un = deux and one + one = two.

Little Chinese Remainder Theorem says $\mathbb{Z}/ab \cong \mathbb{Z}/a$ X $\mathbb{Z}/b$
Ex) $\mathbb{Z}/12 \cong \mathbb{Z}/3$ X $\mathbb{Z}/4$
$\bar{7} + \bar{8} = \bar{3}$ vs. $(\bar{1}, \bar{3}) + (\bar{2}, \bar{0}) = (\bar{0} + \bar{3})$, so it's consistent in this example and in general.

## 10/29

A remark on the Chinese Remainder basis:
$n = ab$ where $a \perp b$. We want:

| | | |
|---|---|---|
| x | 1 | 0 |
| y | 0 | 1 |

We can get $x$ directly if $a$ is small.
Ex) a = 3, b = 20.
We're trying to find $x \equiv 1 \mod 3$ or $x \equiv 0 \mod 20$.
20? No
40? Yes. Therefore, $x = 40$
If you're looking for $x \equiv 1 \mod a$ and $x \equiv 1 \mod b$, then the answer is 1.

### Significance of the Chinese Remainder Theorem

If $\mathbb{Z}n \cong \mathbb{Z}a$ X $\mathbb{Z}b$ "Isomorphic rings. So, composite $\mod n \Leftrightarrow \mod a$ and $\mod b$ even if you don't know them.
E.g. From hw: $n = pq$, where $p \neq q$ and they are both prime.
Let's solve $x^2 \equiv 1 \mod n$
$n = pq$

Ex)11,111,111,111
Let's say I happen to know that $11,111,111,111 = n = pq$ where $p, q$ are two prime integer.
Solve for $x \equiv 1 \mod n$.
There are 4 solutions: 1, -1, 2 tht are myseries.
Let $p = 216649$ and $q = 313239$. These happen to be prime and multiply to 11,111,111,111.
Now, it is feasible to solve. $x \equiv 1 \mod 5$ and $x \equiv 1 \mod p$ and $x \equiv -1 \mod q$.
Another example:
$x^2 \equiv x \mod n$.
In base $n$, $x$ and $x^2$ have same last digit.
$\mod 10 : 0, 1, 5, 6$
First, solve for $\mod p$.
$x^2 \equiv x \mod p$
$x(x-1) \equiv 0 \mod p$
Then, $x \equiv 0 \mod p$ or $x - 1 \equiv 0 \mod p$ by primality lemma.

$\mod n$ has a maximal splitting using the Chinese Remainder Theorem into coprime factors
Ex) n = 180 = 45 * 4 = 9*5*4 (can't go any further because they're all coprime).
As in example, it's the prime power factorization, not prime factorization
$\mathbb{Z}/n \cong \mathbb{Z}p_1$ X $\mathbb{Z}/p_2$ x ... x $\mathbb{Z}/p_n$

A test to solve using this.
How many prime(or coprime) residues are there in $\mod n$?
$(/n)^x$ = set of prime residues = residues with reciprocals = groups
Ex) $(\mathbb{Z}/10)^x = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$
Number of these is $\phi(n) = |(\mathbb{Z}/n)^x|$ or the Euler's phi function.

First, in $\mathbb{Z}/p^k$, e.g. $(\mathbb{Z}/8)^x = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$.

Theorem: (part 1) $\phi(p^k) = (p-1)p^{k-1}$
(part 2) (Using chinese remainder theorem) If $n \equiv p_1^{\phi_1} p_2^{\phi_2} \dots p_k^{\phi_k}$, $x$ has $\frac{1}{x} \mod n \leftrightarrow \frac{1}{x} \mod p_1^{\phi_1} \dots$, so $p(n) = (p_1)(p_2) \dots$
Ex) $n = 60 = 3 * 4 * 5$
If $x$ is a prime residue $\mod 60 \leftrightarrow x$ is prime, etc...

# 10/31

### Euler's phi function

$\phi(n) = |(\mathbb{Z}/n)^x|$ = number of prime residues.
Then, Using Chinese Remainder Theorem:
If $n = p_1^{\phi_1} p_2^{\phi_2} \dots p_k^{\phi_k}$, then $\phi(n) = (p_1 - 1)(p_1^{\phi_1 - 1})(p_2 - 1)(p^{\phi_2 - 1}) \dots (p_k - 1)p_k^{\phi_k - 1}$.
Demote one factor of each prime $p$ to p - 1.
What use is $\phi(n)$. 1) If you pick $\alpha$ in a large range at random, or from,
$P(gcd(\alpha, n) = 1) = \frac{\phi(n)}{n} = \Pi_{p|n} \frac{p-1}{p}$ where $p$ is prime and $P$ is the probability function

Ex) $\phi(43^2 * 41) = 42 * 43 * 40 = (43 - 1) * 43 * (41 - 1)$

Ex) I pick a residue $a \mod 60$ at random. $P(a$ is coprime to 60 )
$P(2 \nmid a) = \frac{1}{2}$
$P(3 \nmid a) = \frac{2}{3}$
$P(5 \nmid a) = \frac{4}{5}$
And Euler's phi formula says these probabilities are independent, so $P(2 \nmid a$ and $3 \nmid a$ and $5 \nmid a) = \frac{1}{2} * \frac{2}{3} * \frac{4}{5}$
Say $n = pq$, $p$ and $q$ are big primes.
To factor $n$, it's enough to find $1 < gcd(n, a) < n$ because Euclidean Algorithm is fast. How well doese this work if $a$ is random?
$P(a \equiv 0 \mod n) = \frac{1}{n}$
$P(gcd(n, a) = 1) = \frac{\phi(n)}{n} = \frac{(p-1)(q-1)}{pq} > 1 - \frac{1}{p} - \frac{1}{q}$.
If $p, q$ are big, this happens almost always.

Theorem (Gauss): If $\phi(n) = 2^k$, then you can build $\cos \pi n$ and $\sin \pi n$ (and even $\cos\left(\frac{2\pi}{n}\right)$ etc...) with only square roots.
Ex) $\sin \frac{\pi}{3} = \frac{\sqrt{3}}{2}$
Ex) $\cos \frac{\pi}{5} = \frac{\sqrt{5}+1}{4} = \frac{\tau}{2}$ where $\tau$ is the golden ratio.

Ex) $\cos \frac{\pi}{4} = \frac{\sqrt{2}}{2}$
Ex) $\cos \frac{\pi}{170} =$ answer is no more complex than a square root.

Primality is easier than factoring.
Fermat's little theorem: If $p$ is prime, then $a^p \equiv a \mod p$. -OR- $a^{p-1} \equiv 1 \mod p$ unless $a \equiv 0 \mod p$.

Ex) $2^7 = 128 \equiv 2 \mod 7$ Does $7|126$? Yes!
$512 = 2^9 \equiv 2 \mod 9$? No. $9 \nmid 510$
Instead, $2^9 \equiv -3 \equiv 6 \mod 9$
If for some $a$, $a^n \equiv a \mod n$, then $n$ is composite.
What do you learn about factors of $n$? Usually NOTHING!
We already have Wilson's theorem, $(p-1)! \equiv -1 \mod p$, also looks like primality test.
It is, but it's slow. $O(p)$ residues computation.( Can be reduced to $O(\log p)$ also
To compute $a^p$ though, takes $O(\log p)$ also.
No one said $a^n \equiv a \mod n \to n$ is prime.
An $n$ like this is on "a-pseudoprime"
Ex) $2^{2047} \equiv 2 \mod 2047$, but $23|2047$
But, primes are more common than psuedoprime and they have salvages.
Buf, proof of Fermat's little theorem.

(orbit proof): $a^p \equiv a$ is clearly so if $a \equiv 0$, so with $a^{p-1} \equiv 1$ when $a \not\equiv 0$.
Recall that $p$ is prime (hypothesis)
What does multiplication by $a$ do? Ex) a = 2, p = 7
$1 \to 2 \to 4 \to 1$. It cycles around the triangle.
$3 \to 6 \to 5 \to 3$.
So, in example, multiplication of a has two orbits of size 3.
Since $3|6 = p - 1$ in example, $a^{p-1} \equiv 1$.

Lemma: In $\mathbb{Z}/p\ \{0\}$, orbits of multiplication by $a$ are all cycles, then all are some size, $s$.
If we know this, we're happy. there are $\frac{p-1}{s}$ of these cycles, so $s|p-1$, so $a^s \equiv 1$.
How could an orbit not have a cycle? It's called a *pho*

# 11/3

## Fermat's Little Theorem

If $p$ is prime and $gcd(a, p) = 1$ or $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. Unlike Wilson's theorem, left side can be computed qiuckly $\to$ on important primality test.

Proof:

Look at $(\mathbb{Z}/p)^x$ = set of prime residues = set of non-zeroes since $p$ is prime.
There are $p-1$ of them. This is the same $p-1$ in the statement of the theorem.
What does $x \mapsto ax$ do if you input it.
If $S$ is any set and $f : S \to S$ is a function, $x_0$, $x_1 = f(x_0)$, $x_2 = f(x_1)$, ... is called an orbit.

What can an orbit be if $S$ is finite?
It can cycle around to anything. It must happen eventually.
The tail of the orbit is the portion of the cycling orbit that is not contained in the cycle.


Lemma: In our situation, $f(x) = ax$ in $\mathbb{Z}/p$ or $f(x) \equiv ax$. The orbits have no tails. They are complete cycles. We cannot have $x_{k-1} \to x_k$ and $x_{n-1} \to x_k$ with $x_{n-1} \neq x_{k-1}$
i.e. if $ax_{k-1} \equiv ax_{n-1} \mod p$, then $x_{k-1} \equiv x_{n-1}$ or if $ax \equiv ay \mod p$, then $x \equiv y \mod p$ because $a^{-1}$ exists $\mod p$, multiply both sides by $a^-1$.

So, $f(x) = ax$ or $f(x) \equiv ax$.
Lemma: All cycles of $x \mapsto ax$ are the same size.
What we have is two starting points $x \in (\mathbb{Z}/p)^x$ and $y \in (\mathbb{Z}/p)^x$ and their orbits
$x \mapsto ax \mapsto a^2x \mapsto \ldots \mapsto a^kx \equiv x$
$y \mapsto ay \mapsto a^2y \mapsto \ldots \mapsto a^ly \equiv y$
Let $k$ and $l$ be the size of the first cycle. We want to show that $k = l$
We want to show that $a^kx \equiv x \leftrightarrow a^ky \equiv y$
This is true! $x^{-1}$ exists and so does $y^{-1}$, so both are equivalent to $a^k \equiv 1$.
This 1st $k > 0$ such that $a^k \equiv 1 \mod p$ is the exponent of a.
Let $e$ = exponent of a
All orbits have this size. $p-1$ prime residue. There are $\frac{p-1}{e}$ is an integer, $e|p-1$.
So, finally $a^{p-1} = (a^e)^{\frac{p-1}{e}} \equiv 1^{\frac{p-1}{e}} \equiv 1 \mod p$.
Ex)a = 2 and p = 7
The residues are the integers between 1 and 6 inclusively.
$1 \mapsto 2 \mapsto 4 \mapsto 1$ and $3 \mapsto 6 \mapsto 5 \mapsto 3$.
They are both of size 3. Well, $p - 1 = 6$ and $e = 3|6$
As a primality test, sometimes even if $n$ is not prime, $a^{n-1} \equiv 1 \mod n$ anyway. We call $n$ a pseudoprime.
But, what if for some composite $n$, most $a's$ prove that it's the composite?
Then, for that $n$, picking random $0 < a < n$ will almost certainly prime $n$ is not prime quickly.
i.e. for $n = 9$, 1 and 8 will certainly yield it.
3 and 6 will certainly fail since they are $0 \mod 9$, so they will never multiply with itself and make $1 \mod 9$.
After trying the rest, you will see that only 1 and 8 will do this.
9 is non-psuedoprime for $\frac{3}{4}$ of its non-zero residues.
Theorem: Say $n$ is composite. Then, $a^{n-1} \not\equiv 1 \mod n$ if $gcd(a, n) > 1$, but there are usually few of these.
Either $a^{n-1} \equiv 1 \mod n \forall a \perp n$ or $a^{n-1} \not\equiv 1 \mod n$ for at least $\frac{1}{2}$ of these residues.
The evil types of $n$ are called Carmichael numbers.
Example: 561 = 3 * 11 * 17
They're rarer than primes, but there are still infinitely many Carmichael numbers.
Fermat's little theorem can be patched up to Miller-Robin primality algorithm.

# 11/5

## Exponents/orders

If $a^3 \equiv 1 \mod n$ for $e > 0$, then the 1st such $e$ is the exponent of $a$. This is also called the order of $a \mod n$.
$a^{e-1} \equiv \frac{1}{a}$. If $a$ has an exponent, it has $a$ reciprocal $\Rightarrow a \perp n$.
If $a \perp n$, then here's a claim: $a$ has an exponent.
Proof: There are only $n$ residues $\mod n$.
$a^0 = 1$, $a^1$, $a^2$, .... Eventually, the powers repeats by the pidgeonhole principle.
So, $a^j \equiv a^k$ for $j > k$, in say $\mod n$.

Then, $a^{-k}a^j \equiv a^{j-k} \equiv a^k a^{-k} \equiv 1 \mod n$.
By Fermat's little theorem, there exists $k$ such that $a^k \equiv 1 \mod n \Leftrightarrow e|k$.
Proof: Multiply by $a$ makes many cycles of length, $e$, and $a^e \equiv 1$. $a^k \equiv 1$ too.

Guarded form of Fermat's little theorem: $a^p \equiv a \mod p$ only to allow $a \equiv 0$.
If $n$ is composite, but $a^n \equiv a \mod n$ for some $a$, then $n$ is a-pseudoprime
If $gcd(a, n) > 1$ and a-pseudoprime from Fermat's little theorem, then $a$ is a lame a-pseudoprime. $a^{n-1} \not\equiv 1 \mod n$ and more $gcd(a, n)$ is computable, shows $n$ is composite and is a factor.
If $a \perp n$ and and a-pseudoprime from Fermat's little theorem, then $n$ is non-lame.
If $n$ is pseudoprime in all non-lame ways, it's a Carmichael number.
They mess up with Fermat's little theorem as a complete primality test.
If $a \perp n$ and $a^{n-1} \equiv 1 \mod n$, then $n$ is non-lame a-pseudoprime. Then, $e$ = exponent of the order of $a$, so their lcm does too.

Definition: If $n$ is a **module**, then its exponent is the lcm of the exponents of its prime residues.
$n$ is Carmichael if its modules exponent, $f|n-1$.
i.e. 561 is Carmichael.
$a^{560} \equiv 1 \mod 561$ if $a \perp 561$.
In fact, $a^{80} \equiv 1 \mod 561$ if $a \perp 561$. 80 is the modulus exponent.
Example:

| | | | | |
|---|---|---|---|---|
| mod 8 | 1 | 2 | 2 | 2 |
| mod 9 | 4 | 5 | 7 | 8 |

So, lcm is 2.

| | | | | |
|---|---|---|---|---|
| mod 8 | 4 | 6 | 7 | 8 |
| mod 9 | 3 | 6 | 3 | 2 |

So, lcm is 6

# 11/7

Definition: The order of $a \mod n$ with $a \perp n$ is the 1st e such that $a^e \equiv 1 \mod n$.
$(\mathbb{Z}/n)^x$ = set of prime residue classes has a maximum order and an lcm order.
A priori: lcms > maxima
Theorem: In $(\mathbb{Z}/n)^x$ or "working mod n", the lcm of the orders is achieved, so lcm-order $\supset$ max-order. Max-order: I'll this this term for 1st $e$ such that $a^e \equiv 1 \mod n$ for all $a \perp n$.
Let $a \perp n$
If $n$ is a pseudoprime $\Leftrightarrow$ $e$, order of $a|n-1$.
If $n$ is Carmichael iff $e$, max-order(= lcm-order) of modulus $n$
$\Rightarrow$ part:
$a^{n-1} \equiv (a^e)^{\frac{n-1}{e}} \equiv 1^{\frac{n-1}{e}} \equiv 1$.
$\Leftarrow$ part:
If $a \perp n$, then $\mod n$, powers of $a$ look like. ($a$ has order $e$).
Then, $a^x \equiv a^y \mod n \Leftrightarrow x \equiv y \mod e$.
Note: The mods are changed.
Note: If $a \equiv b \mod n$, then $a^x \equiv b^x \mod n$.
So, what is the max order of $n$?
If $n$ is prime, then the max order is $n-1$, so there exists a residue $r$ such that $1, r, \ldots, r^{n-1}$ are all prime residues, which are called a primitive residue.

Example: $\mod 7$
1, 10, 100, $10^3, \ldots \equiv 1, 3, 2, 6, 4, 5, \ldots$
Interestingly enough, $\frac{1}{7} = .142857$
If $(\mathbb{Z}/n)^x$ has a prime residue, it's called cyclic.
i.e. 10 is a not prime, it has a prime residue anyway.
Example: 10 is not prime, but it has prime residues anyway. 3,7 are primitive in $\mod 10$
Theorem: (makes things even better) For $\mathbb{Z}/p^k$, if $p$ is an odd prime, it has a primitive residue. $(\mathbb{Z}/p)^x$ is cyclic.
Note: $p = 2$ is different.
For $\mod 8$, $1, 3, 5, 7$ are prime residues.
$3^2 \equiv 5^2 \equiv 7^2 \equiv 1$. Not Cyclic!
Instead, max order of $(\mathbb{Z}/2^k)^x$

$n = 2^k$ is $2^{k-2}$ when $k \geq 3$.
$\phi(2^k) = 2^{k-1}$. max-order is $\frac{1}{2}$ is of this.
For now, mo($n$) = max order of $n$.
Finally,
Theorem: If $a \perp b$ or $a_1, a_2, \ldots a_k$ all are, then mo$(a_1, a_2, \ldots, a_k)$ = lcm( mo($a_1$), mo($a_2$), ..., mo($a_k$))
Example: 561 = 3*11*17
So, mo(561) = lcm(mo(3), mo(11), mo(17)) = lcm(2, 10, 16) = 80
80|560, so 561 is Carmichael.
Example: 1001 = 7 * 11 * 13
so $a^60 \equiv 1 \mod 100$ if $a \perp 1001$, but $a^1000 \equiv a^40 \mod 1001$, which is not always 1 making it not Carmichael.

Theorem: $\exists$ infinitely many Carmichael numbers.
(Proved in 1994)

What is the Miller-Robin primality test for $n$?
Pick a random $a \not\equiv 0$ at random. If $gcd(a, n) > 1$, great!
Otherwise, compute $a^{n-1}$, but leave the pure squaring for last.
Get 1 at end if $n$ is prime (FLT). __ in the pure squaring part, last number before 1 must be -1 if $n$ is prime. And(good part), this quickly (on average) identifies all composites.

# 11/10

mo($n$) - max order $\mod n$ whereas the book has $\lambda(n)$- least universal exponent $\mod n$, least $u > 0$ such that $a^u \equiv 1 \mod n$ when $a \perp n$.
$\lambda(n)$ is also the lcm of orders $\mod n$
Slightly longer theorem; lcm is acheived so that $\lambda(n)$ =mo($n$).

Miller's theorem: If $p$ is prime, then not only is $a^{p-1} \equiv 1 \mod p$, but also, if you save squaring for last, then pure squaring part gives you all 1's or or a-1, then 1's.
Formally, $p - 1 = j2^k$ where $j$ is odd. Then, the form, $a^j, a^{2j}, \ldots, a^{2kj} = a^{p-1} \mod p$.
Then, it is either all 1's or a bunch of stuff, then a -1, and 1s after.
Proof: Each term, $a_l \equiv a_{l-1}^2$, so if $a_l \equiv 1$, then $a_{l-1}^2 \equiv 1 \mod p$. Then, $\pm 1$ are solutions $\mod p$, where $p$ is prime. They're the only solution.

The Irony: Miller's test matters to show primality testing is fast, but it only matters when you get $x^2 \equiv 1$, $x \not\equiv \pm 1 \mod n \Rightarrow$ a factor of $n$.
$n|(x+1)(x-1)$, but $n \not| (x+1)(x-1)$, but $n \not| x+1$ or $x-1$, so that $gcd(n, x \pm 1)$.
If Fermat's little theorem fools for some n. Then, $a^{n-1} \equiv 1 \mod n$, $n$ is an a pseudoprime.
If $a$ and $n$ also passes Miller's test, then $n$ is called a strong a-psudoprime and it does exist.
Ex) $p = 17$, $a = 2$.
$p - 1 = 16 = 2^4 * 1$.
$a^1 = 2, a^2 = 4, a^4 = 16 \equiv -1, a^8 \equiv 1, a^{16} \equiv 1$
Example: n = 2047 = $2^{11}$ - 1 = 11,111,111,111 = a base 2 repeat of prime length = a Merseanwe number.
Miller's test: $2046 = n - 1 = 1023 * 2 = 2 * 11 * 93$
Form: $2^{1023} = (2^{11})^{93} \equiv 1^{93} \equiv 1$, $2^{2046}$, get 1, 1, so two strong 2-pseudoprime
A non-example: 341 is a 20-pseduo prime, but not a strong one.
arithmetic $\mod 341 \Leftrightarrow$ arithmetic $\mod 11$ and $\mod 31$ because $11 \perp 31$ 341 = 11 * 31.
$2^{85}, 2^{170}, 2^{340}$

| | mod 31 | mod 11 |
|---|---|---|
| $(2^5)^{17} = 2^{85}$ | 1 | -1 |
| $2^{170}$ | 1 | 1 |
| $2^{340}$ | 1 | 1 |

They all passed Miller's test in different ways. Then, $2^85 \not\equiv \pm 1 \mod 11 * 31$

Rabin's theorem: If $n$ is composite, then Miller's test proves it for $\geq \frac{3}{4}$ of the residues OR $n$ is a strong a-pseudoprime for $\leq \frac{1}{4}$ of residues $a$.
So, guessing $a$'s at random is a fast probabilistic algorithm.

Chances that $n$ is a composite passes Miller-Rabin 200 times, $\frac{1}{4^{200}} < \frac{1}{10^100}$ such that on $n$ is called a probable prime.

Warmup 0 If $n > 2$ and $2|n$, it's composite.

Warmup 1 Fermat's little theorem is like Miller-Rabin if $n$ is composite, but not Carmichael.
i.e. $n$ is a-pseudoprime for $\leq \frac{1}{2}$ of residues.

# 11/12

If $n$ is composite and is not an a-pseudoprime or is not a strong a-pseudoprime, $a$ is called a "certifcate" or a witness or a proof of "$n$ is composite".
Ex) Theorem: 10001 is composite
Proof: 2 (i.e. $2^{10001-1} \not\equiv 1 \mod 10001$)
In particular, for either test, compositioness is certain.

## Fermat's little theorem test

Either

1. $n$ is prime or Carmichael and no prime residues contradict it
2. $n$ is composite, non-Carmichael, most residues are witnesses are proofs.

## Miller-Rabin test

1. $n$ is prime, no prime residues say otherwise
2. $n$ is composite, most residues are witnesses.

## Is $n$ prime?

Is in $P$ – means can be computation polynomial time with no guesses.
Ex) Is $a \perp b$? Is in $NP$ – means there exists witnesses/proofs that can be checked in polynomial time.
Ex) Is $n$ divisible by a square $> 1$?
Is in $RP$ – like $NP$, but most guesses (of some kind) are proofs.
Ex) The Miller-Rabin test for primality.
$P \subseteq RP \subseteq NP$.
A recent theorem proves that compositeness can be checked in $P$ time.

Let's do the proof for Fermat's little theorem test.
Suppose $n$ is odd, (If $n$ is even, a separate test works anyway!)
What does $a^x \mod n$ look like?
Let $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_l^{k_l}$
Ex) $n = 333 = 9 * 37$ is composite and not Carmichael.
As usually, there's a bijection between $\mod 333$ and $(\mod 37, \mod 9)$. By the Chinese Remainder theorem, $a^x \mod 333 \Leftrightarrow a^x \mod 37$ and $a^x \mod 9$.
Becuase of this, $\mod n \Leftrightarrow \mod p_1^{k_1}, \mod p_2^{k_2} \mod p_3^{k_3} \dots \mod p_l^{k_l}$. $(\mathbb{Z}/p^k)^x$. Then, prime residues is cyclic. If $p$ is an odd prime for $b$ is a primitive residue.
$(\mathbb{Z}/p^k)^x \cong (\mathbb{Z}/\phi(p_k))$
We know that $\phi(p^k) = \lambda(p^k) =$ max order = order of $b$
$x \mapsto b^x$
$+ \mapsto *$
$x + y \mapsto b^x b^y$
Taking $b^x$ to $x$ is called "discrete logarithm".
Ex) $\mod 9$ $b = 2$ is a prime residue. $\log_2 7 \mod 9$ is $4 \mod 6$, which is order of 2
$4 \mod 6$, which is order of 2

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $2^x$ | 1 | 2 | 4 | 8 | 7 | 5 | 1 |

$a^x \mod n \Leftrightarrow a^x \mod p_1^{k_1}, a^x \mod p_2^{k_2}, \dots, a^x \mod p_l^{k_l}$
Then, by discrete logarithm, pick a primitive residue, $b_1, \dots, b_l$.
$a^x \equiv 1 \mod n$, these $x * (\log_{b_1} a)$ iff they are $0 \mod$ whatever $\mod \phi(p_1^{k_1})$.

2 is primitive mod 9.
3 is primitive mod 37 (maybe?!?!?!)

$7^x \mod 2^{4x}$
$7^x \equiv 3^{ex}$ where $e$ can be anything.
$ex \equiv 0 \mod 36$
$4x \equiv 0 \mod 6$ because $7 \equiv 24$.

$e_j \equiv \log_{b_j} a$
$a^x \equiv 1$ when $e_j x \equiv 0 \mod (p_j - 1)(p_j^{k_j - 1} \forall j$.
If $\phi(p_j^{k_j}) | n-1$, then $n$ is Carmichael and $n - 1 = 0 \equiv \phi(p_j^{k_j}$ and $e_j x$ is too.
If $n$ isn't Carmichael, some $\phi(p_j^{k_j} \not| n-1$
When you choose $a$ at random, $\log_{b'_j} a'$ is random too, so how likely is it that $e_j(n-1) \equiv 0 \mod \phi(p_j^{k_j})$ at random? Ex) $n = 333$, $x = n - 1 = 332 \equiv 2 \mod 6$.
$e2 \equiv 0 \mod 6$. How often if $e$ is random? $\frac{1}{3}$ in this case.
$\frac{gcd(n-1,p)}{\phi(p_1^{k_1})} \leq \frac{1}{2}$

# 11/17

Theorem: If $n$ is neither prime nor Carmichael, then $a^{n-1} \not\equiv 1 \mod n$ for more than half of prime residues.
Miller-Rabin: If $n$ is not prime, then it fails Miller's test for more than three-fourths of prime residues.
Lemma(informly): If $n$ has no small factors, prime residues residues. (If $n$ is prime, prime residues = non-zero residues)
From the first theorem today, for $n = pq$ and $p \neq q$ and both prime, then two ideas to this this.

1. chinese Remainder theorem $\mod n \Leftrightarrow \mod p$ and $\mod q$ separately. We will study $a^{n-1}$
2. Multiplication $\mod p \Leftrightarrow$ addition $\mod p - 1$ "index arithmetic" = discrete logarithms

Working $\mod n$ (any $n$) say. $b$ could be a power of $a$. $a, b \perp n$.
Powers of $a$ go in a circle of size $ord_n a$, $b$ is somewhere on the circle, "$\log_a b$" $= ind_{a_n} b$ is where it is, defined $\mod ord_n a$
$a^x * a^y = a^{x+y}$ because both sides are $(a * a * \ldots * a) * (a * a * \ldots * a)$ where the former has $x$ $a$'s and the latter has $y$ $a$'s.
Only subtlety is $x$ and $y$ may only be defined $\mod ord a$.
Analogus in $\mathbb{R}$ or $\mathbb{Z}$.
$(-1)^{\text{odd}} = -1 * (-1)^{\text{even}} = 1$.
And, theorem, if $p$ is prime, $\exists$ a primitive root/ residue $r \mod p$.
$ord r = p - 1$, as long as possible, $1, r, r^2, \ldots r^{p-2}$ are all non-zero residues.
Question was how often is $a^{n-1} \equiv 1 \mod n$? $\Leftrightarrow a^{n-1} \equiv 1 \mod p$ and $a^{n-1} \equiv 1 \mod q$.
$\exists$ prime residues $r \mod p$ and $s \mod q$.
$ind_{r,p} a =$ something $= xa \equiv r^x \mod p$.
$ind_{s,q} a = y$, so $a \equiv s^y \mod q$.
Plug in $r, s$ and take log. $a^{n-1} \equiv 1 \mod n \Leftrightarrow r^{x(n-1)} \equiv 1 \mod p$ and $s^{y(n-1)} \equiv 1 \mod q$
$\Leftrightarrow x(n-1) \equiv 0 \mod p - 1$ and $y(n-1) \equiv 0 \mod q - 1$.
$a$ is flat random (among $a \perp n$) $x, y$ are flat random $\Leftrightarrow$ are flat random.
$x$ is a random residue. How likely is $x * 4 \equiv 0 \mod 7$ and $x * 4 \equiv 0 \mod 6$.
For the former, $\frac{1}{7}$ since $x \equiv 0 \mod 7$. As for the latter, it is equivalent to $x * 2 \equiv 0 \mod 3$, so $\frac{1}{3}$ since $x \mod 0 \mod 3$.
In general, if $x$ is random, $x * a \equiv 0 \mod b$ with chance $\frac{gcd(a,b)}{b}$.
$x(n-1) \equiv 0 \mod p$ with chance, $\frac{gcd(n-1,p-1)}{p-1} = \frac{gcd(pq-1,p-1)}{p-1}$.
say that $p > q$, then I claim that $\frac{gcd(pq-1,p-1)}{p-1} \leq \frac{1}{2}$.
Will happen unless $p - 1 | pq - 1$.
Say $p = 5, q = 17$. $pq = 85$.
$p - 1 = 4$, $pq - 1 = 84$
$p - 1 | pq - 1$ here, so bad!
$16 \not| 84$, then good here. Why does it satisfy? $p > q$.
$pq - 1 = q(p-1) + q - 1$ is the remainder if $p > q$.
Where we stand with algorithms.

| Fast or probably fast | Slow as far as we know |
|---|---|
| gcd, reciprocals mod n, | factoring, primitive residue, discrete logs(ind) |
| primality, exponentiation mod n, existence of quadratic residues | solving quadratic residues |
| whether $ind_r a$ is even or odd | |

Pollar $\rho$ factoring algorithm.
Factors $n$ with some guessing and some conjecture. in time, $O(n^{\frac{1}{4}})$ vs. guessing divisors $O(n^{\frac{1}{2}})$.

# 11/19

## Types of uncertainty in algorithms

Monte-Carlo random: Algorithm is fast, but answer is only probably correct, on one side or both sides. Example: Miller-Rabin, $\tilde{O}(d^2)$ time for primality. No is certain, but yes is only probable.
Las-Vegas style: Answer is definitely right (computer proves the answer), Work is only probably fast. "Elliptic curve primality algorithm".
$\tilde{O}(d^4)$ time (where $d$ is the number of digits in $n$.
Example: Mersenne primes, $2^p - 1$, and Wagstaff primes, $\frac{2^p+1}{3}$
Mersenne primes have a special test. It's as fast as Miller-Rabin, but certain. It's called the Lucas-Lehmer.
Wagstaff primes. No special tes. Known primes up to 20,000 digits. Others are probable primes.

## Primitive roots

Kuperberg said that it's hard to find them, but only sort of. It depends on how hard it is to factor $p-1$. $p$, prime, has alwaysa prime root, but how many?
It has at least 1 in which says $(\mathbb{Z}/p)^x \cong \mathbb{Z}/(p-1)$ Say $r$ is our favorite primitive root.
Then, when is $a \equiv r^x$ another primitive root?
We want to know that $a^k \not\equiv 1$ for $1 \leq k < p-1 \Leftrightarrow kx \not\equiv 0 \mod p-1$, $\bar{x} \in (\mathbb{Z}/p)^x$ and $x \perp p-1$.
There are $\phi(p-1)$ solutions
Usually, $\phi(n) \approx n$ or $\frac{n}{2}$ or so.
So, a lot of residues $\mod p$ are primitive roots.
How do you have find an even one?
We want to know $a^k \not\equiv 1 \mod p$ for $i \leq k < p-1$.
The 1st such $k$ is $ord(a)$ such that $k|p-1$.
Example: p = 101
To check $a$ is enough to check $k|100$, $a^k \equiv 1 \mod 101$ from $k = 1, 2, 4, 5, 10, 20, 25, 50$
You do not need to check all of those either. If we check $k = 20$, we don't need to check for $k = 4$. In fact, you only need to check 20 and 50.
So, actually, $a$ is a primitive root $\mod p$ iff $a^k \not\equiv 1 \mod p$ for maximal proper divisors of $p-1$.
$k = \frac{p-1}{q}$ where $q|p-1$ is a prime.
Note: you must know how to factor $p-1$

## Loose ends

Why $\mathbb{Z}/p$ has a primitive root?
(A standard theorem): If $a(x)$ is a polynomial of degree, $d$, then $a(x) \equiv 0 \mod p$ has at most $d$ roots.
In particular, $a^k \equiv 1 \mod p$ has a subset of $k$ solutions, which implies one big cycle. Example: $i \equiv 2 \mod 5$ or $i \equiv 3 \mod 5$
$x^2 + 1 \equiv 0 \mod 5$ is 2 solutions. $x^2 + 1 \equiv 0 \mod 7$ has no solutions.

Euler's theorem: $\mod$ any $n$. $a^{\phi(n)} \equiv 1 \mod n$ if $a \perp n$
It is proved the same way as Fermat's little theorem.
$(\mathbb{Z}/n)^x$ splits into cycles by multiplying by $a$, all of length $ord_n a$
$\lambda(n)$ is the maximum order or least universal exponent, which is also the lcm of orders. This is where we get $\lambda(n)|\phi(n)$

Pollard $\rho$ factoring algorithm: 1) How do you size an iteration orbit of some $f(x)$. $f$ : some set $\to$ itself or formally, $f : S \to S$, where $S$ is some set.
If we do this, we get a tail of size, $k$, and loop has size $n$.
Naive algorithm: Make $x_0, x_1, \ldots$ and compare $x_k$ to all previous have to compare all pairs up to $x_{n+k}$. This is $O((n+k)^2)$ work. That's slow.
Floyd's cycle-finding algorithm: Find a repetition ($\frac{1}{p}$ with more work, 1st one) in linear time. Make two "people" "run" along orbit, one twice as fast as the other.
Fast runner catches up to detect repetition before slow runner completes. This is $\leq 3(n+k)$ steps total, so $O(n+k)$.

# 11/21

Pollard $\rho$ factoring algorithm continued This is how computers find factors of numbers:

1. $\leq 5$ digits - trial division. Runtime: $\tilde{O}(\sqrt{n}) = \tilde{O}(2^{d/2})$
2. $\leq 10$ digits - Pollard $\rho$ algorithm. Runtime: $\tilde{O}(\sqrt{p}) = \tilde{O}(n^{1/4}) = \tilde{O}(2^{dM})$
3. More digits - Elliptic curve factoring. Runtime: $2^{O(\sqrt{dlogd})}$

If factors of $n$ are about equal (about the same number digits). There's also the quadratic sieve.

Pollard's $\rho$ algorithm:

1. Pick a polynomial (that is NOT linear). For example, $f(x) = x^2 + 1$ is ok. $x^2 + 47$ is often used. $f(x) = x^2$ is a bad choice. In general, they're all usable just that some of it is worse than others.
2. Then, make sequence $\mod n$, an orbit of f. For example, let $x_0 =$ some random number, $x_1 \equiv f(x_0) \mod n$, $x_2 \equiv f(x_1) \mod n, \ldots$.

Stop when it starts looping. If we do not find that $\rho$ shape. Instead look for an $x_j$ such that $x_j \equiv x_k \mod p$ or $\mod q$ where $p$ is a prime factor of $n$ and that gcd unless $x_j \equiv x_k \mod n$ is a factor of $n$.(!)

When this happens, $gcd(x_j - x_k, n) > 1$. $p|n$, $p$ some prime, we seek repetition $\mod p$, we can detect it even though we don't know $p$(!)
$gcd(x_j - x_k, n) > 1$ is the condition.

There is picture $\mod p$
$x_0 \mapsto x_1 \mapsto x_2 \mapsto \ldots \mapsto x_k \mapsto \ldots \mapsto x_n \equiv x_k$

Naive slow way: $x_j \equiv x_k \mod p$ with $j < k$. Compare each $x_k$ with $x_j$ for all $j < k$, compute $gcd(x_k - x_j, n)$
This takes $\binom{k}{2} = O(k^2)$ comparisons.
Faster way: Slow runner $\equiv x_j$ and fast runner $\equiv x_{2j}$

$x_{2j}$ only is good enough because fast runner gains 1 step on show one per iteration passes through O.
Other way: $\leq 3l$ uses of $f$, where l is total orbit mod p.

Issues:
1) Why it works at all? - Rigorous answer
2) How fast usually? Not rigorous. Based on motivated conjectures.

1) If you have a general iteration $\mod n$,
$f : \mathbb{Z}/n \to \mathbb{Z}/n$ defined somehow. There will be nothing consistent $\mod p$.
Say $n = pq$ where $p \neq q$ are prime, then if $f(x)$ is a polynomail.
$\mod n$ $\mod p$ $\mod q$
$x_{j+1} \equiv f(x_j)$ $x_{j+1} \equiv f(x_j)$ $x_{j+1} \equiv f(x_j)$ $f$ splits into something $\mod p$ and $\mod q$ by Chinese Remainder Theorem because Chinese Remainder Theorem preserves addition and multiplication.

2) How fast?
We want to know how big the $\rho$ is $\mod p$. $p$ is the smallest prime factor. Massive non-rigorous assumption: If $f(x)$ is a "typical" polynomial $x_{j+1} \equiv f(x_j \mod p$ will "look random". ("typical", "look random", not rigorous)
Say we could make $f$ random $\mod p$.
$x_0$ - starting point
$x_1 \equiv f(x_0)$ - random
$x_2 \equiv f(x_1)$ - random unless we repeated
$x_3 \equiv f(x_2)$

# 11/24

A loose end in orders of primitive roots mod $p$, prime.
Multiplication mod $p \leftrightarrow$ addition mod $p - 1$.

$a \equiv r^x \leftrightarrow x \equiv ind_r a$ where $r$ is the fixed favorite primitive root. $ord_p a \leftrightarrow$ additive order of $x$. Least $e$ such that $ex \equiv 0 \mod p-1$
Examples: Least $e$ such that $e3 \equiv 0 \mod 10$ is $e = 10$
$e4 \equiv 0 \mod 6$ is $e = 6$
$e2 \equiv 0 \mod 3$ is $e = 3$
So, $e = \frac{p-1}{gcd(x,p-1)} = p-1$ when $x$ is a prime residue.

Also, primitive root $\leftrightarrow$ prime residues

Example: $2^{7^{100000000}} \mod 19$
We want to know $7^{100000000} \mod 18$
$7^3 \equiv 1 \mod 19$ and funnily enough $7^3 \equiv 1 \mod 18$.

## Pollard $\rho$ method

$n$ is the number of factors, say known composites.
$p|n$ is the 1st prime divisor.
$f(x) = x^2 + 1$, say, some polynomial which 1) residues nicely mod $n \to$ mod $p$ (because it's a polynomial). 2) is fake-random mod $p$ based on conjecture.

Let $x_0 \equiv$ something and $x_{k+1} \equiv f(x_k) \mod n$. Compute $gcd(x_{2k} - x_k, n)$ and keep going until it loops.
Picture mod $p$ shows why after a while, $gcd(x_{2k} - x_k, n)) > 1$
Why should the $gcd(x_{2k} - x_k, n) < n$ at this time?
Case 1: $p \neq q$
The $\rho$'s mod $p$, mod $q$ are different sizes. Usually, no part, reason that $x_{2k} \equiv x_k \mod q$ just because $x_{2k} \equiv x_k \mod p$.
How big do you expect $\rho$ to be mod $p$.
If $f$ were random mod $p$ ("fake, but accurate"), then looking at $x_1, \ldots, x_k$, "probability" they all differ is $\frac{p-1}{p} * \frac{p-2}{p} * \ldots * \frac{p-k+1}{p} = B(p,k)$.
$B(p,k)$ is the probability that $k$ people have different birthday in a calendar with $p$ days.
This is known as a Birthday paradox.
Birthday paradox: If $k > \sqrt{p} + 1$, then, $B(p,k) < e^{-\frac{1}{2}} \approx .60653$, so $B(p, \alpha\sqrt{p}) \approx e^{-}$

Trial division takes $\tilde{O}(p)$ work and Pollard $\rho$ takes $\tilde{O}(\sqrt{p})$ work

## Perfect numbers

Definition: $n$ is perfects if $\sum$ proper divisiors of $n = n$
Examples: $6 = 3+2+1$
$28 = 14 + 7 + 4 + 2 + 1$
496 is the next one
Questions:

1. Are there many perfect numbers?
2. Are they all even?

Answers:

1. Yes, iff there are infinitely many Mersenne primes.
2. Yes, but it's a conjecture.

# 11/26

$n$ is perfect means that $n = \sum$ proper divisors (weird name).
Another way to say it, $\sigma(n) = \sum$ all divisors of $n$.
Ex) $\sigma(6) = 6 + 3 + 2 + 1 = 12$
$n$ is perfect means that $\sigma(n) = 2n$
$n$ is overperfect if $\sigma(n) > 2n$

$n$ is underperfect if $\sigma(n) < 2n$ (i.e. prime numbers)
How to compute $\sigma(n)$ or otherwise understand set of divisors.
Use unique factorization. $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \leftrightarrow$ a "bag" or a multiset of primes.
If $d|n$, then $d = p_1^{f_1} \dots p_k^{f_k} \leftrightarrow$ a sub-multiset of the prime factors of $n$ where $0 \le f_j \le e_j$
If for some $f_j = 0$, $p_j^{f_j} = 1$, a ghost factor.
So, $d \leftrightarrow$, a vector of exponnets. $\overrightarrow{f} = (f_1, \dots, f_k)$, use this to organize the set of $d|n$

Ex) $d|3000 = n = 2^3 * 5^3 * 3$, $d = 2^{f_1} * 5^{f_2} * 3^{f_3}$

| $f_1, f_2$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1 | 5 | 25 | 125 |
| 1 | 2 10 | 50 | 250 | |
| 2 | 4 | 20 | 100 | 500 |
| 3 | 8 | 40 | 20 | 1000 |

$d|n$ is a maximal proper divisor with respect to divisibility means $\nexists a$ such that $d|a|n$.
i.e. for 3000, and $d \neq a \neq n$
, they are 1000, 1500, and 600 in general. They are $\frac{n}{p}$ where $p|n$ is prime.
Computing $\sigma(n)$
Example: $n = 1000$
$\sigma(n) = 1 + 5 + 25 + 125 + 2 + 10 + 50 + 250 + 4 + 20 + 100 + 500 + 8 + 40 + 200 + 1000 = (1 + 5 + 25 + 125) * (1 + 2 + 4 + 8) = 56 * 15 = 840$
Definition: A function, $f : \mathbb{Z}^+ \to \mathbb{Z}$ (or to $\mathbb{R}$ or to $\mathbb{C}$, is multiplicative means that $f(ab) = f(a)f(b)$, when $a \perp b$
Example: $\phi(n) =$ number of relatively prime, $\sigma(n) =$ sum of divisors.
Hwo to split up $n$ as much as possible to compute $f$.
$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.
So, $f(n) = f(p_1^{e_1}) f(p_2^{e_2} \dots f(p_k^{e_k})$
The sum of divisors case:
$\sigma(p^e) = 1 + p + p^2 + \dots + p^e = \frac{p^{e+1}-1}{p-1}$
So, $\sigma(n) = \pi_j \frac{p_j^{e_j+1}-1}{p_j-1}$ and $\phi(n) = \pi_j (p_j - 1) p_j^{e_j - 1}$ where $n = p_1^{e_1} \dots p_k^{e_k}$
Other multiplicative functions.
1) $\mu(n) =$ Mobius function $= \begin{cases} 0 & \text{if } n \text{ isn't square free} \\ 1 & \text{if square free and even number of prime factors} \\ -1 & \text{if square-free and odd prime factors} \end{cases}$

Example: $\alpha(n) =$ number of divisors and is multiplicative, but not strongly. $\lambda(n) =$ max order mod $n$ is not multiplicative. By the chinese Remainder theorem, $\lambda(ab) = lcm(\lambda(a), \lambda(b))$ when $a \perp b$.
What is known about $\sigma(n) = 2n$ for perfect numbers, $n$.
Conjecture: There are inifitely many perfect numbers.
Theorem: $n$ is even and perfect iff $n = 2^{k-1}2^{k-1}$ and $2^k - 1$
Real conjecture: There are infinitely many and $2^k - 1$ is prime, Mersenne primes.
Odd Perfect numbers:Conjecture: There are none.
Theorem: If $n$ is odd and perfect, then

1. $n > 10^{300}$
2. $n$ has over 75 prime factors with repeats
3. $n$ has over 9 distinct factors.

Fake-random argument(Pomerance) tht "probability" of any odd perfect $n > 10^300$ is $< 10^{-75}$ or 50.

# 10/1

$f$ is multiplicate if $f(1) = 1$ and $f(ab) = f(a)f(b)$ when $a \perp b$.
$f$ is strongly multiplicative if it's multiplicative and if $f(p^k) = f(p)\ \forall k > 1$. (c.f. completely multiplicative: $f(p^k) = f(p)^k$) multiplicative and strongly multiplicative has some interesting behavior, but completely multiplicative is not that interesting.
Recall, $\phi(n) =$ Euler phi funciton (or the number of prime residues is mulltiplicative.
A modification: $\frac{\phi(n)}{n} =$ Probability(random residue is prime) $= \Pi_{p|n} \frac{p-1}{p}$ - Strongly multiplicative. A useful micro-lemma, If $f, g$ are multiplicative, so are $f(n)g(n)$, $\frac{f(n)}{g(n)}$, $\frac{1}{f(n)}$, etc...
Two new ones, $\sigma(n) = \Sigma$ of divisors of n and $\tau(n) =$ number of divisors of $n$. If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, its divisors make an

$(e_1+1)(e_2+1)\dots(e_k+1)$ box.

Example: $n = 200 = 5^2 2^3$ divisors.

| | | | |
|---|---|---|---|
| 1 | 2 | 4 | 8 |
| 5 | 10 | 20 | 40 |
| 25 | 50 | 100 | 200 |

Then, $\sigma(n) = (\frac{p_1^{e_1+1}-1}{p_1-1})(\frac{p_2^{e_2+1}-1}{p_2-1})\dots\frac{p_k^{e_k+1}-1}{p_k-1}$ and it's multiplicative.

Similar, but easier,

$\tau(n) = (e_1+1)(e_2+1)(e_3+1)\dots(e_k+1)$ is also multiplicative.

Example: $\tau(1,000,000) = \tau(5^6 * 2^6) = 7*7 = 49$ for some prime, $p$.

$n$ is perfect if $\sigma(n) = 2n$.

$n$ is abudant if $\sigma(n) > 2n$.

$n$ is deficient if $\sigma(n) < 2n$.

$n$ is $k$-perfect if $\sigma(n) = kn$.

Example: $\sigma(120) = 360$ is 3-perfect. 2-perfect is the perfect numbers.

Who was bored enough to discover this? Rene Descartes.

Conjecture: $\forall k \geq 3$, there is only finitely many $k$-perfect number.

Vanilla perfect numbers: $\frac{\sigma(n)}{n}$ is also multiplicative and want $\frac{\sigma(n)}{n} = 2$.

$\frac{\sigma(n)}{n} = \pi_j \frac{p_j^{e_j+1}-1}{(p_j-1)p_j^{e_j}}$ if $n = \pi_j p_j^{e_j}$.

$\frac{\sigma(n)}{n} \leq \alpha(n) = \pi_j \frac{p_j^{e_j+1}}{(p_j-1)p_j^{e_j}} = \pi_j \frac{p_j}{p_j-1}$, so strongly multiplicative.

Example: Say prime factors of $n$ are 5,7,11 maybe many times.

$\frac{\sigma(n)}{n} < \alpha(n) = \frac{11}{10}\frac{5}{4}\frac{7}{6} < 2$, so $n$ is deficient.

As $p$ goes up, $\frac{p}{p-1}$ goes down.

So, Theorem: If $2 \not| n$ and $3 \not| n$ and $n$ is perfect, $nhas \geq 4$ distinct prime factors.

If $n$ is even, then $\frac{\sigma(n)}{n} \leq \alpha(n) = \frac{2}{1} *$ other stuff (unless $n = 2^k$) ¿ 2, so even numbers tend to be abundant.

Theorem:(Euclid-Euler) $n$ is even and perfect iff $n = 2^{k-1}(2^k-1)$ and $2^k-1$ is prime (implies that $k$ is prime).

Then, $2^k - 1 = (1111\dots1)_2$, so $(11\dots1)_2 | (11\dots1)_2$

$2^a - 1 | 2^{ab} - 1$

Proof:($\Rightarrow$, Euclid)

$2^{k-1} \perp 2^k - 1$

$\sigma(2^{k-1} = (111\dots1)_2 2^k - 1$

$\sigma(2^k - 1) = 2^k$, so $\sigma(n) = (2^k-1)2^k = 2n$

Example: $n = 31 * 16$

$\sigma(31) = 32$

$\sigma(16) = 16+8+3+2+1 = 31$

so, $\sigma(31*16) = 31*32 = 2*(31*16)$

Proof: ($\Leftarrow$, Euler)

Let $n = 2^s t$, where $t$ is odd, but hypothesis.

$\sigma(n) = 2^{s+1} - 1\sigma(t)$ for $s \geq 1$ by UF, $n = 2^s(2^{s+1}-1)q$. This is odd part from $\sigma(2^s)$ other odd part.

Rest of the argument will be $q = 1$ and $n$ is abudant, then $2^{s+1}$ is prime, or $n$ is abudant.