ITCS 531: Number Theory 1 - Prime numbers

Rob Egrot

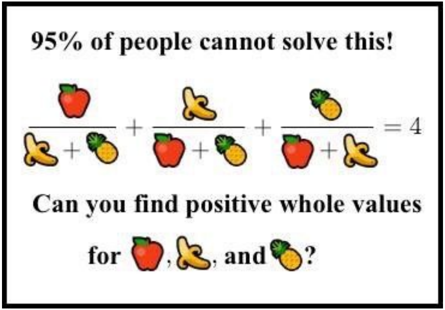
Prime numbers

- Prime numbers the elementary particles of arithmetic.
- I.e. they cannot be divided into smaller pieces, and they are the building blocks for all other numbers.
- Mathematicians have been fascinated by prime numbers for thousands of years.
- There are many simple questions about them that need very advanced techniques from abstract mathematics to solve.

Gaps between primes

- For example, do you know if there are an infinite number of primes p such that $p + 2$ is also prime?
- Nobody does (this is the *twin prime conjecture*).
- First proved there is *any* finite number k with an infinite number of pairs of primes whose difference is less than k in 2013.
- The first proof by Yitang Zhang has k around 70,000,000, but this has been reduced to 246.
- More relevant in computer science, prime numbers and their properties give us important techniques for encryption.

Digression - fruit



Digression - solution

- Simplest solution:

apple = 154476802108746166441951315019919837485664325669565431700026634898253202035277999
banana = 36875131794129999827197811565225474825492979968971970996283137471637224634055579
pineapple = 4373612677928697257861252602371390152816537558161613618621437993378423467772036

- Brute force search will fail.
- Need heavy mathematics.
- More at: `https://www.quora.com/How-do-you-find-the-integer-solutions-to-frac-x-y+z-+-frac-y-z+x-+-frac-z-x+y-4/answer/Alon-Amit`.

Notation for sets

- $\mathbb{N}$ is the set **natural numbers**, so $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- $\mathbb{Z}$ is the set of **integers**, so $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- $\mathbb{Q}$ is the set of **rational numbers**. $\mathbb{Q}$ can be thought of as the set of fractions of two integers.
- $\mathbb{R}$ is the set of **real numbers**. $\mathbb{R}$ can be thought of as the set of all numbers expressible as a (possibly infinite) decimal.
- Every real number that is not rational is **irrational**.
- If X is a set and x is an element, we use $x \in X$ to say that x is a member of X.

What is a prime number?

- Given two integers $a, b \in \mathbb{Z}$, we say a divides b if there is $c \in \mathbb{Z}$ with $b = ac$.
- We write $a \mid b$ if a divides b.
- If a does not divide b we write $a \nmid b$.

Definition 1 (Prime number)

$n \in \mathbb{N}$ is *prime* if $n > 1$ and, whenever $a, b \in \mathbb{N}$, if $ab = n$ then either $a = 1$ and $b = n$ or vice-versa.

- We use $\mathbb{P}$ for the set of prime numbers.
  - So $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$.
- Numbers that are not prime are **composite**.

What is to be done

In this class we will prove two important results about prime numbers which were known to the ancient Greeks.

Theorem 2 (Fundamental Theorem of Arithmetic)

Every natural number greater than 1 can be expressed as a product of primes. Moreover, this product is unique up to reordering.

Theorem 3

The set of prime numbers is infinite.

We will need some facts about numbers

Digression - why prove?

- Modern mathematicians are obsessed with proof.
- This goes back to the Ancient Greeks, e.g. as seen in e.g. Euclid.
- Some Greeks had a religious interest in mathematics (e.g. Pythagoras and his school).
- Other earlier cultures applied mathematics, e.g. in Egypt, Mesopotamia, China.
- But these cultures did not emphasize theoretical proof over observation.
- So why is proof so valued today?

Digression - the road to modern mathematics

- This is actually a modern phenomena.
- Although Western mathematics is inspired by Ancient Greece, till the mid 19th century proofs were often not rigorous at all.
- As math becomes more complicated, more precision is needed for understanding.
- Also, even easy to understand things that look true turn out to be false.
- E.g. “there are no positive integers a, b, c such that $\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} = 4$”.
- Experiments with ‘small’ numbers will tell you this is true, but we know it is false.

Division of sums

Lemma 4

Let $a, b_1, \ldots, b_n \in \mathbb{Z}$. Then, if $a|b_i$ for all $i \in \{1, \ldots, n\}$, we have $a|(b_1 + \ldots + b_n)$.

Proof.

- For each $i \in \{1, \ldots, n\}$ there is k_i with $b_i = k_i a_i$ (by definition of $a|b_i$).
- So $b_1 + \ldots + b_n = k_1 a + \ldots + k_n a = (k_1 + \ldots + k_n)a$.
- And so $a|(b_1 + \ldots + b_n)$ as claimed.

□

- Is the converse true?
- I.e. if $a|(b_1 + \ldots + b_n)$ is it always true that $a|b_i$ for all $i \in \{1, \ldots n\}$?
- No. e.g. $2|(1 + 3)$, but 2 doesn't divide either 1 or 3.

Another lemma

Lemma 5
Let $a, b, c \in \mathbb{Z}$. Then if $a|b$ and $a|(b+c)$ then $a|c$.

Proof.

- By definition there are $x, y \in \mathbb{Z}$ with $xa = b$ and $ya = b + c$.
- So combining these we get $ya = xa + c$.
- And so $(y - x)a = c$, and so $a|c$ by definition.

$\square$

Yet another lemma

Lemma 6

Given $a, b \in \mathbb{N}$ with $a < b$, if c is the highest common factor of a and b, then c is also the highest common factor of $b - a$ and a.

Proof.

- By definition there are $x, y \in \mathbb{N}$ with $xc = a$ and $yc = b$.
- So $(y - x)c = b - a$, and so $c|(b - a)$.
- I.e. c is a common factor of $b - a$ and a, and we must show it is the largest such factor.
- If $d|(b - a)$ and $d|a$, then by lemma 4 we must have $d|b$.
- And so $d \leq c$ as c is the highest common factor of a and b.
- So c is the highest common factor of $b - a$ and a as required.

$\square$

The Euclidean algorithm

Proposition 7 (Euclid's algorithm)

Given $a, b \in \mathbb{N}$ with $a < b$ we can find $\mathbf{HCF}(a, b)$ by computing:

$$
\begin{aligned}
b &= x_0 a + r_0 \text{ where } r_0 < a \\
a &= x_1 r_0 + r_1 \text{ where } r_1 < r_0 \\
r_0 &= x_2 r_1 + r_2 \text{ where } r_2 < r_1 \\
&. \\
&. \\
&. \\
r_{n-3} &= x_{n-1} r_{n-2} + r_{n-1} \text{ where } r_{n-1} < r_{n-2} \\
r_{n-2} &= x_n r_{n-1} + r_n \text{ where } r_n < r_{n-1} \\
r_{n-1} &= x_{n+1} r_n
\end{aligned}
$$

In which case the HCF is r_n.

The Euclidean algorithm - proof

- The algorithm must terminate, because $r_i < r_{i-1}$, so at some point must reach zero.
- r_0 is found by subtracting a from b multiple times.
- So, if c is the HCF of a and b, then it is also the HCF of a and $b - a$, and of a and $b - 2a$ etc. (lemma 6).
- So also of a and r_0, as $r_0 = b - x_0 a$.
- By the same logic, the HCF of a and r_0 must also be the HCF of r_0 and r_1.
- Continuing this thought process we see that the HCF of a and b must also be the HCF of r_{n-1} and r_n.
- This can only be r_n, as $r_n < r_{n-1}$.

The Euclidean algorithm - another proof

- r_n divides r_{n-1}.
- So r_n also divides r_{n-2} (lemma 4).
- Similarly r_n divides r_{n-3} etc.
- So $r_n|a$ and $r_n|b$.
- If $d|a$ and $d|b$ then $d|r_0$ (lemma 5).
- Similarly $d|r_1$ etc.
- So $d|r_n$.
- I.e. r_n is HCF of a and b.

The extended Euclidean algorithm

Corollary 8 (Bézout's identity)

If $a, b \in \mathbb{N}$ and $\mathbf{HCF}(a, b) = d$, then there are $x, y \in \mathbb{Z}$ such that $d = xa + yb$.

Proof.

- Use Euclid's algorithm in reverse.
- Start with $d = r_n = r_{n-2} - x_n r_{n-1}$ in the last step and work backwards.
- E.g. the first two steps of this calculation give us:

$$\begin{aligned} r_n &= r_{n-2} - x_n r_{n-1} \\ &= r_{n-2} - x_n(r_{n-3} - x_{n-1} r_{n-2}). \end{aligned}$$

- Define $b = r_{-2}$, and $a = r_{-1}$.
- For all i we replace r_i with a term containing r_{i-1} and r_{i-2}.
- We end up with only a and b, and no other r_i values.

$\square$

Division by primes

Lemma 9

Let $p \in \mathbb{P}$ and let $a, b \in \mathbb{N} \setminus \{0\}$. Then, if $p|ab$, either $p|a$ or $p|b$.

Proof.

- Suppose $p|ab$ and $p \nmid a$.
- Then $\mathbf{HCF}(p, a) = 1$, so by corollary 8 there are $x, y \in \mathbb{Z}$ with $xp + ya = 1$.
- But since $xp + ya = 1$ it follows that $xpb + yab = b$, and since $p|xpb$ and $p|yab$, by lemma 4 we must have $p|b$.
- A similar argument proves that if $p \nmid b$ then we must have $p|a$.

$\square$

This result generalizes to $p|a_1 \dots a_n \implies p|a_i$ for some $i \in \{1, \dots, n\}$. You can prove this using induction.

Almost ready

- We are almost ready to prove theorems 2 and 3.
- We just need one more idea.

The well-ordering principle

Lemma 10 (Well-ordering principle)

If $X \subseteq \mathbb{N}$ and $X \neq \emptyset$, then X has a smallest element. In other words, every non-empty subset of natural numbers has a smallest member.

Proof.

- Since X has at least one element we can pick $x \in X$.
- X has a finite number of elements less than or equal to x.
- One of these must be smaller than all the others.

$\square$

Induction

- The well-ordering principle is essentially mathematical induction.
- I.e. From "true for 0" and "true for n implies true for $n + 1$" conclude "true for all natural numbers".
- Well-ordering says that if a statement is *not* true for some natural number, then there must be a smallest natural number k where it is not true.
- To apply well-ordering usually prove that it's impossible for this smallest k to exist for some statement.
- Then can conclude that the set of natural numbers for which the statement of interest is true is empty.
- I.e. the negation of the statement is true for all natural numbers.

Proving theorem 2

- There are two parts to this.
- Existence: we must show that for all $n > 1$ a prime factorization exists.
- Uniqueness: we must show that any two prime factorizations of n must be the same up to reordering.
  - E.g. $2 \times 7 \times 2 \times 5$ is a reordering of $2 \times 2 \times 5 \times 7$.

Proving existence

- Suppose $n \in \mathbb{N}$ and has no prime factorization.
- Then by the well-ordering principle suppose n is the smallest such number.
- If n is prime then n is its own prime factorization (contradiction).
- So n is composite.
- But then $n = ab$ for some non-trivial factors a and b.
- By minimality of n, both a and b have prime factorizations.
- These combine to give a prime factorization of n.
- I.e. if $a = p_1 \dots p_k$ and $b = q_1 \dots q_m$ then $n = p_1 \dots p_k q_1 \dots q_m$.
- Contradiction.

Proving uniqueness

- Suppose n has 2 distinct factorizations as $p_1 \dots p_k$ and $q_1 \dots q_m$.
- By well-ordering we assume that n is minimal with this property.
- Here p_i and q_j are primes (which may be repeated) for all $1 \leq i \leq k$ and $1 \leq j \leq m$.
- p_1 is not equal to q_i for any $i \in \{1, \dots, m\}$.
    - Otherwise we could divide both factorizations by p_1 to obtain a number smaller than n.
    - But unique factorization would fail for this new number.
    - This would contradict minimality of n.
- But $p_1 | n$, and so $p_1 | q_1 \dots q_m$.
- So by lemma 9 we must have $p_1 | q_j$ for some j.
- As q_j is prime this means $p_1 = q_j$, which cannot happen.

Proving theorem 3

- Suppose there are only a finite number of primes.
- Let the set of primes is $\{p_1, \ldots, p_n\}$.
- Then consider the number $k = (\prod_{1=1}^{n} p_i) + 1$.
- By the existence part of theorem 2 we know there must be a prime number p dividing k.
- Since $\{p_1, \ldots, p_n\}$ contains all the primes we must have $p = p_j$ for some $j \in \{1, \ldots, n\}$.
- But $p_j | k$ and $p_j | \prod_{i=1}^{n} p_i$.
- So by lemma 5 we must have $p_j | 1$.
- Contradiction.
- So the set of primes must be infinite.