

Number Theory & Proving "Real" Theorems: Part II

Basics of Number Theory

Number theory was once thought to be “pure” mathematics – math for the sake of math. But with the evolution of computers (and particularly cryptography), number theory has become known as an applied area of math. Much cryptology relies on some very old theorems from number theory.

What is number theory? It is the branch of mathematics that studies problems about natural numbers, integers and rational numbers, i.e., anything but real numbers. It was invented by the Greeks. Number theory is a subject in which the concepts are simple but the problems can be quite challenging. We choose to work with number theory for two reasons in 103A: a) The simple axioms and definitions in number theory allow us to focus on proof techniques and not get distracted; b) Number theory has many important applications in CS.

We assume for our purposes that you understand what integers are (negative and positive whole numbers including 0), and what the natural numbers are (positive integers > 0). Note that there is no agreement among mathematicians as to whether to include 0 in the set of natural numbers. We will not include it. We also assume that you understand and accept as valid the basic arithmetic operations. The slides from today's lecture discuss these points in more detail.

The integers are *closed* under addition, subtraction and multiplication, meaning if we add/subtract/multiply an integer and another integer, we get an integer. The integers, however, are not closed under division, which sets division apart from other operations. We can still consider “div” an integer operation if we define it in a special way. (Note: where proofs are not given and not covered in lecture, you are encouraged to find your own.)

Definition: If a and b are integers and $a \neq 0$, then the statement that a divides b means that there is an integer c such that $b = ac$. Our notation for “ a divides b ” is $a \mid b$.

Theorem 32.1: For all integers a , b , and d , if $d \mid a$ and $d \mid b$ then $d \mid (a \pm b)$

Theorem 32.2: For all integers a , b , and c , if $a \mid b$ then $a \mid bc$.

Proof: Suppose $a \mid b$, then there exists an integer k such that $ak = b$. Since $(ak)c = bc$, we can conclude that $a \mid bc$, since there exists an integer (kc) such that $a(kc) = bc$. Q.E.D.

Theorem 32.3: For all integers a , b , and c , if $a \mid b$ and $b \mid c$ then $a \mid c$.

The divisibility definition leads us to the Division Theorem, which is an elegant term for something you have known since elementary school. We can perform division working only with integers if we introduce the notion of a remainder:

The Division Theorem

Let a be an integer and let d be a positive integer. Then there exist unique integers q and r , with $0 \leq r < d$ such that $a = dq + r$. r is called the *remainder of a divided by d* and q is called the *quotient*. This theorem is often called the Division Algorithm.

One of the oldest (yet still useful) applications of the Division Theorem is in finding greatest common divisors.

Definition: Suppose a and b are integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b . We denote this as $d = \gcd(a, b)$. If $\gcd(a, b) = 1$, then a and b are said to be *relatively prime*.

For example, 12 and 18 have common divisors 1, 2, 3, and 6 with $\gcd(12, 18) = 6$. $\gcd(4, 15) = 1$ which means 4 and 15 are relatively prime (but note that they are not prime numbers).

How do we find $\gcd(a, b)$? Brute force would work – just start at the smaller of a and b , and work your way down to 1 checking each number to see if it evenly divides a and b . This would be very slow if a and b are large or if they are relatively prime. A much better method exists called Euclid's Algorithm, which first appeared in Euclid's Elements (≈ 2300 years ago).

The algorithm rests on the fact that if r is the remainder of a divided by b , $\gcd(a, b) = \gcd(b, r)$ (which we will prove in a minute).

Suppose we want to compute $\gcd(315, 54)$. Apply the division theorem to obtain

$$315 = 54 \cdot 5 + 45.$$

If we assume that $\gcd(a, b) = \gcd(b, r)$, then $\gcd(315, 54) = \gcd(54, 45)$. Apply the division theorem again to get $54 = 45 \cdot 1 + 9$. Now we have

$$\gcd(315, 54) = \gcd(54, 45) = \gcd(45, 9)$$

Once more apply the division theorem to obtain $45 = 9 \cdot 5 + 0$. When we get a remainder of 0, we are done:

$$\gcd(315, 54) = \gcd(54, 45) = \gcd(45, 9) = \gcd(9, 0) = 9$$

In the algorithm shown below, $a \bmod b$ means the remainder of a divided by b .

Euclid's Algorithm: (assume a and b not both 0)

```

gcd(a, b)
{
  if a = 0 return |b|
  if b = 0 return |a|
  repeat
  {
    r := a mod b
    a := b
    b := r
  } until r = 0
  return a
}

```

Why is $\gcd(a, b) = \gcd(b, r)$?

Theorem 32.4: If $a = bq + r$ and a, b, q, r are integers, then $\gcd(a, b) = \gcd(b, r)$.

Proof: If we can show that the common divisors of a and b are the same as the common divisors of b and r then we have shown that $\gcd(a, b) = \gcd(b, r)$ since both pairs must have the same *greatest* common divisor. So we will prove a more general result than the theorem requires.

Suppose $d \mid a$ and $d \mid b$. It follows from our proofs a couple pages back that d divides bq and d also divides $a - bq$. Notice that $a - bq = r$. So any common divisor d of a and b also divides r . We can conclude from this that any common divisor of a and b is also a common divisor of b and r .

Likewise, suppose that $d \mid b$ and $d \mid r$, then d also divides $bq + r$ (using our proofs again). Notice that $a = bq + r$. So any common divisor of b and r is also a common divisor of a and b .

Consequently, $\gcd(a, b) = \gcd(b, r)$. Q.E.D.

One more property of $\gcd()$ will be useful later when we study cryptography:

Theorem 32.5: If $\gcd(a, b) = d$ then we can find integers m and n such that $d = am + bn$. This is called the *gcd identity* or *Bézout's Identity*.

For example, $\gcd(110, 42) = 2$ and we can write $2 = 110 \cdot -8 + 42 \cdot 21$. We say that we can write 2 as a *linear combination* of 110 and 42. Euclid's Algorithm provides the means for finding m and n , all we have to do is work backwards and substitute. For example, $\gcd(252, 198) = 18$. We can express 18 as a linear combination of 252 and 198 by first applying Euclid's algorithm:

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \end{aligned}$$

$$\begin{aligned}54 &= 36 \cdot 1 + 18 \\36 &= 2 \cdot 18\end{aligned}$$

Using the next to last equation we can solve for 18:

$$18 = 54 - 1 \cdot 36$$

Going back to the second equation and solving for 36:

$$36 = 198 - 3 \cdot 54$$

Now substitute the equation for 36 into the equation for 18:

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$

Finally, the first equation shows us that $54 = 252 - 1 \cdot 198$ which we substitute in the above equation:

$$18 = 4 \cdot 54 - 1 \cdot 198 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$

$m = 4$, and $n = -5$.

Prime Numbers

Definition: The statement that an integer $n > 1$ is *prime* means that for all positive integers r and s , if $n = rs$, then $r = 1$ or $s = 1$. The statement that an integer $n > 1$ is *composite* means that $n = rs$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Theorem 32.6: If p is prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$ then the conclusion is true. Suppose it does not – we need to show that $p \mid b$. Let d be a common divisor of p and a . Since p is prime, d must be either p or 1 . We have assumed that p does not divide a , so $d = 1$. The gcd identity tells us that there exist integers m and n such that $1 = am + pn$. Multiplying by b we have $b = abm + pbn$. Since $p \mid ab$ and $p \mid pbn$, then $p \mid (abm + pbn)$. Thus, by substitution, $p \mid b$. Q.E.D.

We can generalize this to:

Theorem 32.7: If p is prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i .

We think of the prime numbers as basic building blocks in number theory due to the following theorem.

Fundamental Theorem of Arithmetic:

Every positive integer greater than 1 is either prime or equal to the product of two or more prime numbers. Moreover, if the primes are written in nondecreasing order, this factorization is unique.

We need induction to prove both parts of this theorem. We need to prove that the factorization is possible and we also need to prove this factorization is unique. We'll do this when we study induction in a week or two. The factorization is often written like this, where $n > 1$, p_1, \dots, p_k are distinct primes in increasing order, and e_1, \dots, e_k are positive integers:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Example: $8100 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3^4 \cdot 5^2$

Just because we can prove a factorization exists does not mean it is easy to find. In fact, factoring is a very difficult problem and is the focus of much recent work in cryptography. The security of the RSA encryption technique (which we will study soon) depends on factoring being a time-consuming activity. If someone discovers a quick method, then this technique would no longer be useful, at least in its current form.

There is a simple algorithm for determining if a number is prime or composite. It is shown below, using the following definitions:

Given any real number x , the *floor* of x , denoted $\text{floor}(x)$, and the *ceiling* of x , denoted $\text{ceil}(x)$, are defined as follows:

$\text{floor}(x)$ = that unique integer n such that $n \leq x < n+1$ (i.e. the largest integer not larger than x).

$\text{ceil}(x)$ = that unique integer $n+1$ such that $n < x \leq n+1$ (i.e. the smallest integer not smaller than x).

In the algorithm, please forgive the C-like notation for the "for loop." It means: start a at 2, execute the loop in curly brackets as long as $a \leq \text{floor}(\text{sqrt}(n))$, and add 1 to a after each loop execution.

```

Prime(n)      assume n is an integer > 1
{
    for (a := 2, a ≤ floor(sqrt(n)), a++)
    {
        if ((n mod a) = 0)
        {
            return FALSE
        }
    }
    return TRUE
}

```

This algorithm is not too useful if n is large – we need other methods for such numbers. By the way, why do we stop at $\text{floor}(\text{sqrt}(n))$?

Theorem 32.8: If n is composite, then n has a prime divisor less than or equal to $\text{sqrt}(n)$.

Modular Arithmetic

We have used the mod operator a couple times now without formally defining it. Mod is an important part of number theory.

Definition: If a and b are integers with $b > 0$ then the remainder upon the division of a by b is denoted $a \bmod b$.

If we agree to fix b as a positive integer, then $a \bmod b$ takes values from the set $\{0, 1, 2, \dots, b-1\}$ which is the set of possible remainders obtained upon division of any integer a by b .

We have a notation that we use to indicate that two integers have the same remainder when they are divided by some positive integer m .

Definition: If a and b are integers and m is a positive integer, then a is said to be *congruent* to b modulo m if m divides $(a - b)$. We use the notation $a \equiv b \pmod{m}$ to indicate a is congruent to b modulo m . Later we will prove that $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Is 17 congruent to 3 modulo 2? Just check if 2 divides $17 - 3$, which it does. Also note that $17 \bmod 2 = 5 \bmod 2$.

More Theorems

Several useful theorems are shown below. It's important to notice the form we have used in doing proofs in this handout. We are still being quite formal, but we are leaving some simple steps out. You should use these proofs as a model for those you do on the problem set.

Theorem 32.9: If $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$.

Proof: Since $\gcd(d, a) = 1$, we can use the gcd identity: there exist integers m and n such that $1 = dm + an$. Multiply both sides by b to obtain $b = bdm + ban$. Note that $d \mid bdm$ and $d \mid ban$. Since d divides both terms on the right side of the equation, d also divides the left side and therefore $d \mid b$. Q.E.D.

Theorem 32.10: If $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.

Proof: By the gcd identity there exist integers m and n such that $1 = am + bn$. Multiply both sides by c to obtain $c = cam + cbn$. From the divisibility assumptions, there exist integers s and t such that $as = c$ and $bt = c$. Substituting for c in the previous equation gives
 $c = btam + asbn = ab(tm + sn)$. Thus $ab \mid c$. Q.E.D.

Theorem 32.11: If $x = 2^k$ for some positive integer k , and y is an odd integer, then x and y are relatively prime.

Proof by contradiction: Suppose x and y are not relatively prime. Therefore, $p = \gcd(x, y)$ and $p > 1$. Then p must be a power of 2 greater than 1 because $x = 2^k$, and $y = pq$ for some integer $q > 1$. That means p is an even number. The product of an even number (p) with

any other number must be even so y must be even. This is a contradiction, so x and y must be relatively prime. Q.E.D.

Theorem 32.12: $x \bmod n = y \bmod n$ iff $n \mid (x - y)$ iff $(x - y) \bmod n = 0$

Proof in one direction: From the Division Theorem, there exist integers $q_1, r_1, q_2,$ and r_2 such that

$$x = nq_1 + r_1, \text{ where } 0 \leq r_1 < n \text{ and}$$

$$y = nq_2 + r_2, \text{ where } 0 \leq r_2 < n$$

Using the definition of modulus,

$$x \bmod n = r_1 = x - nq_1 \text{ and}$$

$$y \bmod n = r_2 = y - nq_2$$

Suppose $x \bmod n = y \bmod n$. Then

$$r_1 = r_2$$

From the equations above

$$x - nq_1 = y - nq_2 \text{ and}$$

$$x - y = n(q_1 - q_2)$$

Since n divides the right hand side, it must also divide the left; i.e.,

$$n \mid (x - y)$$

Thus the remainder of $x - y$ divided by n is 0, which we write as

$$(x - y) \bmod n = 0$$

The proof in the other direction is left as an exercise for the reader.

Theorem 32.13 Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$.

Proof: if $a \equiv b \pmod{m}$, then $m \mid (a - b)$. This means there is an integer k such that $a - b = km$ or $a = b + km$. Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Thus, $m \mid (a - b)$ giving us $a \equiv b \pmod{m}$. Q.E.D.

Some Famous Conjectures

There are many conjectures that have never been proven or disproven, and some that have taken a long time to be decided. Some famous ones:

1) Goldbach's Conjecture: If n is an even integer > 2 , then n can be represented as the sum of two primes.

Note that $4 = 2+2, 6 = 3+3, 8 = 5+3, 10 = 5+5, 12 = 7+5,$ etc. No one has proven this, but computer calculations show this is true for all integers up to 10^{18} .

2) Euler's conjecture that $a^4 + b^4 + c^4 = d^4$ has no integer solution. This was accepted as true for 200 years until it was proven wrong by one counterexample:

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

(It was also proven wrong formally by Elkies at Harvard)

3) Fermat's Last Theorem: It is impossible to find positive integers x, y, z such that $x^n + y^n = z^n$ for $n \geq 3$ (there are solutions for $n = 2$ e.g., $3^2 + 4^2 = 5^2$)

Fermat wrote this theorem in the margin of a book he was reading about 350 years ago. He wrote beside it: "I have discovered a truly remarkable proof of this theorem which this margin is too small to contain." This was one of the most famous open questions in mathematics until recently when it was proven by Andrew Wiles of Princeton.

There will always be open conjectures in mathematics. Gödel's Incompleteness Theorem states that it is not always possible to find a proof for every true statement in a mathematical system. Thus, we may never be able to establish whether certain conjectures are actually true.

Original handout by Maggie Johnson; modified by Robert Plummer