Number Theory Notes

Math Circle Competition Team

October 22nd, 2017

Source: Andre Kessler, Contest Number Theory

Notation

- When we write $a \mid b$, we mean that a **divides** b, as in there exists an integer c such that $a = bc$. For example, $3 \mid 12$. If a does not divide b, then we write $a \nmid b$. An example would be $3 \nmid 11$.
- $\gcd(a, b)$ denotes the **greatest common denominator** of a and b, which is the largest integer that divides both numbers. This is usually abbreviated to (a, b). Example: $(12, 20) = 4$.
- The **least common multiple** of two numbers is the smallest number that they both divide. This is written $[a, b]$, and an example would be $[12, 20] = 60$.
- $\mathbb{N}$ means the natural numbers, $\mathbb{Z}$ the integers, $\mathbb{Z}^+$ the positive integers, $\mathbb{Z}/n\mathbb{Z}$ the integers $\pmod n$, $\mathbb{Q}$ the rational numbers, $\mathbb{R}$ the real numbers, and $\mathbb{C}$ the complex numbers.
- n, m, and k are commonly used as integers. p and q are usually primes. If we want a variable, we usually use x, y, and z, with w and z often used for complex numbers. Constants are often a, b, and c. i, j, and k are often indices or dummy variables. f and g are quite often functions. Roots of unity are usually something like ω or ξ.

The Theorems

Modular Arithmetic

Consider a number system in which we replace each number with its remainder on division by some fixed integer n. Well, this is a perfectly valid system in which to do arithmetic! We call this arithmetic "modulo n", or $\pmod n$. As you may have seen above, we denote the integers $\pmod n$ as $\mathbb{Z}/n\mathbb{Z}$. Let's consider some examples of arithmetic in $\mathbb{Z}/5\mathbb{Z}$:

$24 \equiv 4 \pmod 5$
$3 + 4 \equiv 2 \pmod 5$
$12 \cdot 23121321789321378912285 \equiv 12 \cdot 0 \equiv 0 \pmod 5$

As you can see, we have a nice system. But watch out! You can't cancel multiplication all of the time. Why? Because $x \equiv 0 \pmod n$ does not mean $x = 0$, and we can have

$xy \equiv 0 \pmod{n}$ even if neither x nor y is zero. An example of this is $20 \equiv 2 \pmod{6}$, but $10 \not\equiv 1 \pmod{6}$. What happened?

Consider a number a that divides the product of two others: $a \mid bc$. Clearly a can be split into parts a_0 and a_1 such that $a_0 a_1 = a$, $a_0 \mid b$, and $a_1 \mid c$. Importantly, if p is a prime, the only way to split it into two parts is $p \cdot 1$. Thus if $p \mid bc$, then $p \mid b$ or $p \mid c$.

By the definition of $a \mid bc$, we have that $ka = bc$ for some integer k, so $k = \frac{bc}{a} = \frac{b}{a_0}\frac{c}{a_1}$ for a_0 and a_1 that divide b and c. This means that both $\frac{b}{a_0}$ and $\frac{c}{a_1}$ are integers, and thus $\frac{b}{a_0} \mid \frac{bc}{a}$. But since a_0 divides both a and b, it divides (a, b). Thus $\frac{b}{(a,b)} \mid \frac{b}{a_0}$, leading us to the conclusion that

$$\frac{b}{(a,b)} \mid \frac{bc}{a} \tag{1}$$

Let's now look at the general case. We have

$$ac \equiv bc \pmod{n} \tag{2}$$

This means that ac and bc differ by some number nk for some k. This means that a and b differ by $\frac{nk}{c}$, which must be an integer, and so $c \mid nk$. By (1), we have that $\frac{n}{(n,c)} \mid \frac{nk}{c}$. Thus $a - b = \frac{nk}{c}$ which means $a - b \equiv 0 \pmod{n/(n,c)}$, and (2) becomes

$$a \equiv b \pmod{n/(n,c)} \tag{3}$$

Going back to our previous example, we have

$$20 \equiv 2 \pmod{6} \Rightarrow 2 \cdot 10 \equiv 2 \cdot 1 \pmod{6} \Rightarrow 10 \equiv 1 \pmod{6/(6,2)} \Rightarrow 10 \equiv 1 \pmod{3} \tag{4}$$

Note that from this we have $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$ iff $(n, c) = 1$.

Prime Mods

Prime mods are nice because we *can* cancel multiplication in them. This is clear because if we use our canceling equation (3), we note that (p, c) will be 1 since p is prime, so we have $ac \equiv bc \pmod{p} \Rightarrow a \equiv b \pmod{p}$, as long as c is not a multiple of p. This is because if $p \mid c$, then $c \equiv 0 \pmod{p}$ and our equation before would be meaningless.

We can do more. Since $ac \not\equiv bc$ unless $a \equiv b$, we know that the sequence

$$\{0, a, 2a, 3a, \ldots, (p-1)a\} \tag{5}$$

consists of all residues $\pmod{p}$. Thus it is a permutation of the set

$$\{0, 1, 2, 3, \ldots, p-1\}.$$

Now we get to an interesting idea. Notice that the set (5) will always contain one element that is 1 $\pmod p$. Thus for every non-zero a, we can find some number b such that $ab \equiv 1$. What other number system is this like? More on this later.

Fermat's Little Theorem

If we take the powers of some number $a \not\equiv 0 \pmod p$, the numbers a^2, a^3, etc. cannot all be different, since they are all between 0 and $p-1$. Thus two must be the same, so let's say $a^j = a^k$. Then if we let $j > k$, we have $a^{j-k} \equiv 1 \pmod p$. Thus the powers of a with be 1 at some point, and we call the least number $ord(a) \pmod p$ (the order of $a \pmod p$), or $ord_p(a)$ for short.

Now consider what we said above when we talked about $\{0, a, 2a, 3a, \ldots, (p-1)a\}$ being a permutation of $\{0, 1, 2, 3, \ldots, p-1\}$. This means that we can say

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

canceling $1 \cdot 2 \cdot 3 \cdots (p-1)$ from both sides leaves

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

This very important theorem is known as **Fermat's Little Theorem**.

Fermat's Little Theorem 1. For any integer a and any prime p,

$$a^p \equiv a \pmod p \tag{6}$$

Euler's Totient and Generalization

Let's try to find an analog of Fermat's Little Theorem for $\pmod n$, where we let n be any integer instead of only primes. Notice we will only be able to cancel numbers from both sides the way we did when n was prime if the number being canceled is relatively prime to n. In addition, a will have to be relatively prime to n (do you see why?). Let $S = \{1, k_0, k_2, \ldots, n-1\}$ be the set of all integers less than and relatively prime to n. We can do something similar to what we did before, namely

$$a \cdot k_0 a \cdot k_1 a \cdots (m-1)a \equiv 1 \cdot k_0 \cdot k_1 \cdots (n-1) \pmod n$$

We need a way to count the numbers less than and relatively prime to n. Therefore, we define a function $\varphi(n)$ that returns the desired number. This is known as **Euler's totient function**. Now we can do what we did before and cancel $1 \cdot k_0 \cdot k_1 \cdots (n-1)$ from both sides, yielding

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

This is known as **Euler's generalization** of Fermat's Little Theorem.

Euler's Generalization 1. For any relatively prime integers a and n,

$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{7}$$

Wilson's Theorem

Wilson's Theorem 1. For any odd prime p,

$$(p-1)! \equiv -1 \pmod{p} \tag{8}$$

Remember that in any prime mod, a number a has a unique inverse that we'll call a^{-1} such that $aa^{-1} = 1$. We use this fact in the proof of Wilson's Theorem.

Proof. Consider $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1)$. Let's write the final element as -1, since obviously $p - 1 \equiv -1 \pmod{p}$. Notice that -1 is its own inverse. In this it is unique: every other element a (except 1, of course) will have a distinct inverse such that $aa^{-1} = 1$, so we can replace all of these element-inverse pairs with ones. We now have $1 \cdot 1 \cdots 1 \cdot -1 \equiv -1$, and thus we have proven Wilson's Theorem. □