# Contest Number Theory

Andre Kessler

December 17, 2008

## 1 Introduction

Number theory is one of the core subject areas of mathematics. It can be somewhat loosely defined as the study of the integers. Unfortunately, most grade school mathematics curricula don't cover number theory at all, leaving students clueless about a highly fascinating subject. Because of this, most contest problems involving number theory are relatively easy to people that have a decent grasp of the theory. Basic number theory itself is actually very simple, and number theoretic problems are often very easy to understand. Advanced number theory can get trickier, and the best way to get a good intuition about such problems is to practice a lot. And then, of course, you have the insane unsolved problems. Have you ever heard of Fermat's Last Theorem? It states that there are no positive integer solutions to $x^n + y^n = z^n$ for $n > 2$. This problem remained open for 357 years.

## 2 Notation

If there's something in this section you don't understand, don't worry, it will be explained in its respective section. This is mainly intended as a reference.

- 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, $\mathbb{Q}'$ the irrational 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 $\omega$ or $\xi$.
- $\phi : F \to F'$ means that $\phi$ is a mapping from $F$ to $F'$.
- $\Leftrightarrow$ means **iff** means **if and only if**.
- $A \Rightarrow B$ means **if** $A$, **then** $B$.
- s.t is **such that**.
- $\sum_{d|n}$ means a sum over all the divisors $d$ of $n$.

# 3 The Theorems

## 3.1 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 sysem to do arithmetic in! 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 $(n, c) = 1$.

### 3.1.1 Exercises

1. Evaluate $(1440983213234)^{123321} \pmod 5$.
2. Prove that if $ab$ is a perfect square and $(a, b) = 1$, then both $a$ and $b$ must be perfect squares.
3. Solve the congruence $1232x \equiv 9045 \pmod{24}$

## 3.2 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

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

Make sure you understand this. This idea comes up everywhere in number theory.

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.

## 3.3 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 3.3.1.** *For any integer $a$ and any prime $p$,*

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

## 3.4 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 3.4.1.** *For any relatively prime integers $a$ and $n$,*

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

### 3.4.1 Exercises

1. Explain why (7) is considered a generalization of Fermat's Little Theorem.
2. Calculate $\varphi(12)$.
3. Find the units digit of $4^{4^{4^4}}$.
4. Find $\varphi(p^k)$ for $p$ prime and any positive integer $k$.
5. Prove that $\varphi$ is **multiplicative**, that is, $\varphi(mn) = \varphi(m)\varphi(n)$ if $m$ and $n$ are relatively prime.
6. From the result of the two earlier problems, find an explicit formula for $\varphi(n)$, $n$ being any positive integer.

## 3.5 Wilson's Theorem

**Wilson's Theorem 3.5.1.** *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. □

### 3.5.1 Exercises

1. Prove that the function $F(j) = \left\lfloor \cos \pi \dfrac{(j-1)! + 1}{j} \right\rfloor$ returns 1 when $j$ is prime and 0 when $j$ is composite.

## 3.6 Divisor Sums

There is a useful formula for the number of the divisors of a number. If the prime factorization is

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

then the number of the divisors of $n$, $\tau(n)$, is

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1) \tag{9}$$

Since the proof of (9) is pretty easy and rather well known, let's turn it into an exercise in summation notation.

*Proof.* We are seeking the number of divisors of $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Note that our desired result is equivalent to

$$\sum_{d|n} 1$$

Now, look at the following nested sum. Can you see how this is equivalent to the previous sum?

$$\sum_{i_1=0}^{e_1}\sum_{i_2=0}^{e_2}\cdots\sum_{i_k=0}^{e_k}1$$

Now, the solution is simple. We break apart the nested sum, and obtain the formula.

$$\begin{aligned}\tau(n) &= \sum_{i_1=0}^{e_1}\sum_{i_2=0}^{e_2}\cdots\sum_{i_k=0}^{e_k}1 &(10)\\ &= \left(\sum_{i_1=0}^{e_1}1\right)\left(\sum_{i_2=0}^{e_2}1\right)\cdots\left(\sum_{i_k=0}^{e_k}1\right) &(11)\\ &= (e_1+1)(e_2+1)\cdots(e_k+1) &(12)\end{aligned}$$

□

Once we've derived the formula for the number of divisors, it is very easy to obtain a formula for the *sum* of the divisors, $\sigma(n)$. All it takes is to realize that

$$\begin{aligned}\sigma(n) &= \sum_{d|n}d &(13)\\ &= \sum_{i_1=0}^{e_1}\sum_{i_2=0}^{e_2}\cdots\sum_{i_k=0}^{e_k}p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k} &(14)\\ &= \left(\sum_{i_1=0}^{e_1}p_1^{i_1}\right)\left(\sum_{i_2=0}^{e_2}p_2^{i_2}\right)\cdots\left(\sum_{i_k=0}^{e_k}p_k^{i_k}\right) &(15)\\ &= (1+p_1+p_1^2+\cdots p_1^{e_1})(1+p_2+p_2^2+\cdots p_2^{e_2})\cdots(1+p_k+p_k^2+\cdots p_k^{e_k}) &(16)\end{aligned}$$

It is clear that we can extend this to the sum of the $k^{\text{th}}$ powers of the divisors, $\sigma_k(n)$. This result is left as an exercise to the reader.

It's best to use these formulas to appreciate them. So, let's find the number and then the sum of the divisors of 666. We know that $666 = 2\cdot 3^2\cdot 37$. Thus $\tau(666) = (1+1)(2+1)(1+1) = 12$. Now we plug the numbers into the divisor sum formula.

$$\sigma(666) = (1+2)(1+3+9)(1+37) = 3\cdot 12\cdot 38 = 1368$$

### 3.6.1 Exercises

1. Find the sum of the divisors of the sum of the divisors of 1000.
2. Make the formula for $\sigma(n)$ simpler using the formula for the sum of a geometric sequence.
3. A number is perfect if the sum of its divisors (excluding itself) is equal to itself. The first three are 6, 28, and 496. Prove that any number of the form $2^k(2^{k+1}-1)$ is perfect if $2^{k+1}-1$ is prime.
4. Extend the above proof to show that all *even* perfect numbers are of the form $2^k(2^{k+1}-1)$.

## 3.7 Prime Number Facts

There are an infinite number of primes. Why? Well, if there were a finite number of them, they would make a finite set

$$\{2, 3, 5, \ldots, p_n\}$$

But if that was so, $2 \cdot 3 \cdot 5 \cdots p_n + 1$ would have no "prime" factors at all, which is a contradiction. Thus there are an infinite number of primes.

**Dirichlet's Theorem 3.7.1.** *If there is more than one prime in an infinte arithmetic progression, then the arithmetic progression contains an infinite number of primes.*

Proving Dirichlet's theorem in the general case is very difficult, however, so there isn't a proof here.

**Green-Tao Theorem 3.7.1.** *There are arbitrarily long arithmetic progressions of primes.*

This is also very difficult and was only recently proven.

**Bertrand's Postulate 3.7.1.** *There is always a prime $p$ such that for any $n > 1$, $n < p < 2n$.*

Bertrand's postulate is more accurately called **Chebyshev's Theorem**, because it was only postulated by Bertrand, whereas Chebyshev proved it. This is also takes too long to prove, even though the proof is relatively elementary.

If you ever are trying to solve a problem, and your solution hinges on the truth of one of the following conjectures, it's best to try something else. These have remained unsolved for decades or centuries .

**Goldbach Conjecture 3.7.1.** *Every even integer greater than 2 can be written as the sum of two primes.*

**Twin Prime Conjecture 3.7.1.** *There are infinitely many primes $p$ such that $p + 2$ is also prime.*

**Mersenne Prime Conjecture 3.7.1.** *There are infinitely many primes of the form $M_n = 2^n - 1$.*

**Palindromic Prime Conjecture 3.7.1.** *There are infinitely many primes that are palindromic; that is, they are the same if their digits are reversed.*

**Conjecture 3.7.1.** *$an^2 + bn + c$ is prime for infinitely many values of $n$, as long as $a$, $b$, and $c$ are pairwise relatively prime.*

## 3.8 Diophantine Equations

A **diophantine equation** is an equation in which we are interested in only integer solutions. Bézout's Identity is the solution to a relatively easy Diophantine equation. When solving diophantine equations, you have to keep one thing in mind: you cannot just give a bunch of answers. You have to show they work, and that no other answers exist.

**Steps to Solve a Diophantine Equation**

1. Write out the answers to the problem. In the case of, say, $x + y = 0$, you would write $(n, -n)$ for $n \in \mathbb{Z}$.
2. Show that your answers work.
3. Prove that you have given all the answers. Usually, this requires a bit of number theory.

**Methods for Solving Diophantine Equations**

- Take the equations in certain mods. For example, if you see squares, mod4 is good, since all squares are 0 or 1. If you see cubes, try mod9, since cubes are -1, 0, and 1. Mod 8 is good for squares a well.
- Factor everything possible!
- Substitution
- Add conditions. If the equation is symmetrical, like $a^2 + b^2 + c^2 = (a + b + c)!$, state that without a loss of generality, $a \geq b \geq c$.
- Infinite descent. This is where you assume an equation has solutions, and you consider the solution whose value is the smallest. Then, show there is another solution whose value is smaller-which is a contradiction, and thus there can be no solutions.

Random important thing to know: the general primitive Pythagorean triple is given by $(2rs, r^2 - s^2, r^2 + s^2)$.

# 4 Problems

The only way you will get better is by doing problems, especially hard problems. SO DO THEM. Harder problems are marked with a ⋆. If you would like to know if your solution is correct, you can email me at apkessler (at) gmail (dot) com.

1. (*AHSME 1973*) Show that for all prime numbers $p$ greater than 3, 24 divides $p^2 - 1$ evenly.
2. (*Mandelbrot #2*) Find the last three digits of $9^{105}$.
3. (*1st IMO Problem, 1959*) Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every positive integer $n$.
4. (*AHSME 1969*) For any integer greater than 1, how many prime numbers are there greater than $n!+1$ and less than $n!+n$?
5. Determine, in terms of $a$ and $n$, how many distinct values the sequence $\{a, 2a, 3a, \dots\}$ takes on $\bmod n$.
6. (*Leningrad 1984*) Find all prime unordered pairs such that $a^b + b^a$ is prime.
7. (*AIME 2006*) Find the least positive integer such that when the first digit is removed, the resultant integer is $\frac{1}{29}$th as large.
8. (*MA*Θ) What is the units digit of $7^{7^7}$?
9. Find the last three digits of $7^{9999}$.
10. (*AOPS vol. 2*) Find all integer solutions to the equation $x^3 + 117y^3 = 5$
11. (*USAMTS 1*) Let $x$ and $y$ be integers such that $2x + 3y$ is a multiple of 17. Show that $9x + 5y$ must also be a multiple of 17.
12. (*M&IQ, 1991*) Prove that for all positive integers $k$, $k^5 - k$ is a multiple of 10.
13. (*Traditional*) Let $p = 4k + 1$ be a prime. Prove that $p \mid k^k - 1$
14. (*AoPS vol. 2*) Prove that the diophantine equation $x^3 + y^3 + z^3 + x^2y + y^2z + z^2x + xyz = 0$ has no solutions in nonzero integers.
15. (*Canada 1976*) Prove that a positive integer is the sum of at least two consecutive positive integers if and only if it is not a power of two.
16. (*Traditional*) ⋆ Prove that there are infinitely many composite numbers in the sequence 1, 31, 331, 3331, ...
17. ⋆ Prove that for all odd integers $k$, $1 + 2 + 3 + \cdots + n \mid 1^k + 2^k + 3^k + \cdots + n^k$
18. (*Engel*) ⋆ Prove that there are infinitely many powers of 2 in the sequence $a_n = \lfloor n\sqrt{2} \rfloor$
19. ⋆ The $n^{\text{th}}$ cyclotomic polynomial is denoted $\Phi_n(x)$, and is defined to be $\Pi(x - \zeta)$ ($\zeta$ ranges over all the primitive $n^{\text{th}}$ roots of unity). Prove that all cyclotomic polynomials are irreducible and that all of their coefficients are integers.
20. ⋆ (*1995 SL/N1*) Let $k$ be a positive integer. Prove there are infinitely many perfect squares of the form $n2^k - 7$ where $n$ is a positive integer.
21. (*Andre Kessler*) ⋆ Let ${}^k a = \underbrace{a^{a^{\cdots^a}}}_{k \text{ times}}$. Prove that the last $n$ digits of ${}^k a$ will become constant for sufficiently large $k$. Find the exact integer $k$ in terms of $n$ after which the last $n$ digits become constant.

This lecture is a work in progress; many more problems will be added eventually.