# NUMBER THEORY

ARTHUR BARAGAR

ABSTRACT. The following are a number of topics in number theory which might help with some Olympiad type problems. I have included several past Olympiad problems at appropriate places. This is not to say that the methods described below are all you need. Quite often, some cleverness is still required.

## CONTENTS

## 1. THE EUCLIDEAN ALGORITHM

You are probably familiar with the *division algorithm*. This says that given $a$ and $b$, there exists a $q$ (the quotient) and an $r$ (the remainder) such that $0 \leq r < q$ and

$$a = bq + r.$$

Of a similar nature is the *Euclidean algorithm*. We call $d = \gcd(a, b)$ the *greatest common divisor* of $a$ and $b$ if $d > 0$, $d$ divides both $a$ and $b$,

LaTeXed June 25, 1998.

and if $c$ also divides both $a$ and $b$, then $c$ divides $d$. We can also define $d$ as follows:

$$d = \min\{ax + by > 0 : x, y \in \mathbb{Z}\}.$$

Check to make sure that these define the same thing. In particular (and this is often useful), there exist integers $x$ and $y$ such that

$$\gcd(a, b) = ax + by.$$

Given $a$ and $b$, we can solve for $x$ and $y$ via the Euclidean algorithm. This is just a repeated use of the division algorithm, and is easiest to demonstrate using a numerical example. So, let us find $x$ and $y$ given $a = 23$ and $b = 13$:

$$\begin{aligned} 23 &= 1 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

We can turn this around:

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (13 - 10) \\ &= 4 \cdot 10 - 3 \cdot 13 \\ &= 4 \cdot (23 - 13) - 3 \cdot 13 \\ &= 4 \cdot 23 - 7 \cdot 13. \end{aligned}$$

Thus, $x = 4$ and $y = -7$.

The Euclidean algorithm also plays a role in some very famous puzzles. For example, explain how to measure exactly 4L of water, given a jug which holds exactly 3L and another which holds exactly 5L (and of course, neither of which has any markings.) Do you see how the Euclidean algorithm plays a role in the solution?

**Exercise.** ('59, #1) Prove that the fraction $\dfrac{21n + 4}{14n + 3}$ is irreducible for every natural number $n$.

## 2. Modular Arithmetic

You again are probably familiar with modular arithmetic, but let us review some definitions. We say two numbers $a$ and $b$ are equivalent (mod $m$) if $m$ divides $a - b$. We sometimes write $[a]$ for the class of elements equivalent to $a$ modulo $m$, so

$$[a] = \{b : m \text{ divides } (b - a)\}.$$

Then, for any integer $a$ there exists an integer $b$ such that $[a] = [b]$ and $0 \leq b < m$. Thus, the set $\{[0], ..., [m-1]\}$ is a complete set of *representatives* modulo $m$. We write

$$\mathbb{Z}/m\mathbb{Z} = \{[0], ..., [m-1]\}.$$

We often drop the brackets and just write

$$\mathbb{Z}/m\mathbb{Z} = \{0, ..., m-1\}.$$

In modular arithmetic, addition and multiplication are exactly as expected. That is, we define

$$\begin{aligned} [a]+[b] &= [a+b] \\ [a][b] &= [ab]. \end{aligned}$$

Check that these definitions are well defined. That is, that it doesn't matter which representative we choose. We will no longer use the square bracket notation, and assume that it'll be clear when we mean an integer and when we mean the class represented by that number.

2.1. **Multiplicative Inverses.** We will call a number $b$ the inverse of $a$ modulo $m$ if

$$ab \equiv 1 \pmod{m}.$$

Note that $a$ is invertible if and only if $\gcd(a, m) = 1$. Suppose that $d = \gcd(a, m)$. Then there exist $x$ and $y$ such that

$$d = ax + my$$

so we have

$$ax \equiv d \pmod{m}.$$

In particular, if $d = 1$, then $a$ is invertible. Now, if $a$ is invertible then there exists $b$ such that

$$ab \equiv 1 \pmod{m}.$$

That is, $m$ divides $ab - 1$. That is, there exists $y$ such that

$$\begin{aligned} ym &= ab - 1 \\ 1 &= ab - my. \end{aligned}$$

Hence, $1 = \gcd(a, m)$.

2.2. **Groups.** The notion of a group is something you'll learn about in the future, but there's really no reason to not introduce them here:

**Definition.** A *group* $G$ is a set of elements together with a relation $\cdot$ (which we'll write as multiplication) such that for any $a$, $b$, and $c$ in $G$, we have

1. $ab \in G$ (closure)
2. $(ab)c = a(bc)$ (associativity)
3. There exists an identity 1 such that for all $a \in G$,
$$a1 = 1a = a.$$
4. For every $a$ there exists an element $a^{-1}$ such that
$$aa^{-1} = a^{-1}a = 1.$$

If we further have $ab = ba$, then we call $G$ an Abelian or commutative group. In the above definition, we represented the relation as a product. We could also write a relation as an addition, but we usually only do so if the relation is commutative. If we use the notation $+$, then we'll also call the identity 0 instead of 1.

Note that $\mathbb{Z}/m\mathbb{Z}$ forms a group where the relation is addition.

We write

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\}.$$

Note that $(\mathbb{Z}/m\mathbb{Z})^*$ is a group under multiplication.

More familiar examples of groups are the integers under addition; the rationals not including zero under multiplication; the rationals under addition, etc.

A related concept is that of a field:

**Definition.** A *field* $F$ is a set of elements together with two relations $+$ and $\cdot$ with the properties that $F$ is a commutative group under $+$; $F\backslash\{0\}$ is a commutative group under multipliction; and for all $a$, $b$ and $c$ in $F$,

$$a(b + c) = ab + ac.$$

This last property is called the *distributive law.*

Familiar examples of fields are the rational numbers; the real numbers; and the complex numbers.

Note that if $p$ is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. If $m$ is not a prime, then $\mathbb{Z}/m\mathbb{Z}$ is not a field.

### 2.3. Fermat's Little Theorem, Euler's Theorem, and Gauss' Lemma.

**Theorem 2.1** (Fermat's Little Theorem). *Suppose $p$ is a prime. Then for all $a$ not divisible by $p$, we have*

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

*Proof.* Consider the set $\{1, ..., p-1\}$ and the set $\{a, 2a, ..., (p-1)a\}$. Note that these two sets are equal, modulo $p$ (why?). Thus,

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$

Now, just 'cancel' the $(p-1)!$ (that is, multiply both sides by its inverse.) □

**Definition.** The Euler phi function is

$$\varphi(m) = \#\{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\}.$$

Euler generalized Fermat's result:

**Theorem 2.2** (Euler's Theorem). *Suppose* $\gcd(a, m) = 1$. *Then*

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

... And Gauss generalized that:

**Theorem 2.3.** *Suppose $G$ is a finite group with $n$ elements, and $a \in G$. Then*

$$a^n = 1.$$

It is often useful to know that if $G$ is a finite group with $n$ elements, $a \in G$, and $m$ is the smallest positive integer such that $a^m = 1$, then $m$ divides $n$. (Prove this.)

### 2.4. The Euler phi function.

The Euler phi function has some interesting properties:

1. If $p$ is a prime, then $\varphi(p^r) = p^{r-1}(p-1)$.
2. If $m$ and $n$ are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

One usually uses the Chinese remainder theorem to prove this last result:

**Theorem 2.4** (Chinese Remainder Theorem). *Let $m$ and $n$ be relatively prime, and let $a$ and $b$ be any integers. There exists a unique $x$ such that $0 \leq x < mn$ such that*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

Though this theorem is stated for two equivalence relations, it generalizes to any number of equivalence relations.

2.5. **Polynomials in modular arithmetic.** Suppose $P(x, y)$ is a polynomial with integer coefficients. Suppose $P(x, y) = 0$ has no solutions modulo $m$ then $P(x, y)$ has no solutions in the integers. Note that this test does not work the other way. Also, there is no point in testing $P(x, y)$ modulo $m$ except for $m$ prime. Of course, there's nothing special about a polynomial in two variables – there could be more or less.

Another useful fact about polynomials is this: A polynomial $P(x)$ factors uniquely into irreducible polynomials modulo $p$. This may not seem too surprising, bu note that this is not true modulo $m$ for $m$ a composite number.

**Exercise.** ('62, #1) Find the smallest number $n$ which has the following properties:

1. Its decimal representation has 6 as the last digit.
2. If the last digit 6 is erased and placed in front of the remaining digits, the resulting number is four times as large as the original number $n$.

**Exercise.** ('64, #1) (a) Find all positive integers $n$ for which $2^n - 1$ is divisible by 7. (b) Prove that there is no positive integer $n$ for which $2^n + 1$ is divisible by 7.

**Exercise.** ('75, #4) When $4444^{4444}$ is written in decimal notation, the sum of its digits is $A$. Let $B$ be the sum of the digits of $A$. Find the sum of the digits of $B$. (Both $A$ and $B$ are written in decimal notation.)

**Exercise.** ('82, #4) Prove that if $n$ is a positive integer such that the equation

$$x^3 - 3xy^2 + y^3 = n,$$

has a solution in integers $(x, y)$, then it has at least three such solutions. Show that the equation has no solutions in integers when $n = 2891$.

**Exercise.** ('84, #2) Find one pair of positive integers $a$ and $b$ such that:

1. $ab(a + b)$ is not divisible by 7;
2. $(a + b)^7 - a^7 - b^7$ is divisible by $7^7$.

Justify your answer.

## 3. The Gaussian integers

We define the complex numbers $\mathbb{C}$ to be

$$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$$

where $i^2 = -1$. We can define a similar object

$$\mathbb{Q}(i) = \{a + ib : a, b, \in \mathbb{Q}\}.$$

This is a generalized notion of the rationals, and is called a number field. We can think of both these objects as vector spaces over respectively the reals and rationals. A set of basis vectors in both cases is $\{1, i\}$.

There is also a generalized notion of the integers in $\mathbb{Q}(i)$. This is the set

$$\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\},$$

and is called the *Gaussian integers.*

In the integers $\mathbb{Z}$, there are only two *units* $\{\pm 1\}$. These are the numbers in $\mathbb{Z}$ whose multiplicative inverses are also in $\mathbb{Z}$. In the Gaussian integers, the group of units is $\{\pm 1, \pm i\}$. (Check that this really is a group.) We are familiar with the definition of a prime number in $\mathbb{Z}$, but let me give a slightly different definition: We call a number $p \in \mathbb{Z}$ (or $\mathbb{Z}[i]$) a prime if the only numbers which divide $p$ are the units and numbers which differ from $p$ by a multiple of a unit.

In the Gaussian integers, just like in the integers, we can factor any number uniquely (up to order and units) into a product of primes.

A very useful map in $\mathbb{Z}[i]$ is the *norm* map:

$$N(a + ib) = (a + ib)(a - ib) = a^2 + b^2.$$

Note that if $\alpha, \beta \in \mathbb{Z}[i]$, then

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Note also that the norm of any Gaussian integer is an integer. Thus, if $N(\alpha)$ is a prime in $\mathbb{Z}$, then $\alpha$ is a prime in $\mathbb{Z}[i]$.

**Theorem 3.1.** *Suppose $p$ is an odd prime (that is, a prime not equal to 2). Then $p$ can be written as the sum of two squares if and only if $p \equiv 1 \pmod 4$.*

The 'only if' is clear since $a^2 + b^2 \equiv 3 \pmod 4$ has no solutions. The 'if' part is not so easy. A consequence of this is that this gives us a way of deciding how many ways a number can be written as the sum of two squares.

For example, can 77 be written as the sum of two squares? The answer is 'no', since if it could, then we could write

$$77 = a^2 + b^2 = (a + ib)(a - ib).$$

This gives a factorization of 77 in $\mathbb{Z}[i]$. But we have another factorization:

$$77 = 7 \cdot 11.$$

Since factorization is unique (I must stress that we haven't proved this, and it is a very important property), and these two factorizations are different, we must have that at least one of 7 and 11 is not prime. But both are, since neither can be written as the sum of two squares.

Here's another example: In how many ways can 65 be written as the sum of two squares? To answer this, we factor $65 = 5 \cdot 13$ in the integers. We now factor each of these in $\mathbb{Z}[i]$:

$$65 = (1+2i)(1-2i)(3+2i)(3-2i).$$

Thus, there are two ways of writing 65 as a sum of two squares. The first is given by

$$(1+2i)(3+2i) = -1+8i$$

and hence $65 = 1^2 + 8^2$. The other is given by

$$(1+2i)(3-2i) = 7+4i$$

and hence $65 = 7^2 + 4^2$.

**Exercise.** ('77, # 5) Let $a$ and $b$ be positive integers. When $a^2+b^2$ is divided by $a+b$, the quotient is $q$ and the remainder is $r$. Find all pairs $(a,b)$ such that $q^2 + r = 1977$.

## 4. Quadratic integer rings

The Gaussian integers are not the only generalization of the integers. It is the generalization associated to the irreducible quadratic $x^2+1$. For example, we could instead define a ring associated to the irreducible quadratic $x^2-2$:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

The norm map is this time

$$N(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2.$$

Unlike the Gaussian integers, the equation

$$N(a+b\sqrt{2}) = a^2 - 2b^2 = \pm 1$$

has an infinite number of solutions. For example, $1+\sqrt{2}$ is a solution, and therefore, so is

$$(1+\sqrt{2})^k$$

for any positive integer $k$. Since this number is clearly greater than 1, these numbers are all different for each $k$. Thus, the group of units is infinite. These solutions, the solutions $(1-\sqrt{2})^k$ for $k$ positive, and the solutions obtained by multiplying these by $-1$ are infact all the solutions. Note that $(1-\sqrt{2})=(1+\sqrt{2})^{-1}$. Thus, the group of units is

$$\{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}.$$

If a quadratic has complex roots, then the group of units is finite, and if the quadratic has real irrational roots, then the group of units is $\{\pm\omega^k : k \in \mathbb{Z}\}$ for some *fundamental unit* $\omega$.

**Remark:** In the example above, we again have unique factorization into primes. This is not always the case. For example, $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization, since

$$6 = 2\cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5}),$$

and neither product factors further. The assumption that one always has unique factorization lead to some famous erroneous proofs of Fermat's Last Theorem.

**Exercise.** ('81, # 3) Determine the maximum value of $m^2+n^2$ where $m$ and $n$ are integers satisfying $m,n \in \{1,2,...,1981\}$ and $(n^2-mn-m^2)^2=1$.

## 5. Independence over $\mathbb{Q}$

A very important fact about these objects is the notion of independence. For example, if

$$a+b\sqrt{2}=c+d\sqrt{2},$$

then $a=c$ and $b=d$. There are some very cute problems which use this fact.

**Exercise.** ('74, # 5) Prove that the number $\sum_{k=0}^{n}\begin{pmatrix} 2n+1 \\ 2k+1 \end{pmatrix} 2^{3k}$ is not divisible by 5 for any integer $n \geq 0$.

## 6. Cyclotomic polynomials and DeMoivre's Theorem

**Theorem 6.1** (DeMoivre's Theorem).

$$e^{i\theta}=\cos\theta+i\sin\theta.$$

This theorem can be used to prove the angle sum formulas:

$$\begin{aligned} \cos(\alpha+\beta) \quad + & \quad i\sin(\alpha+\beta) \\ = & \quad e^{i(\alpha+\beta)} \\ = & \quad e^{i\alpha}e^{i\beta} \\ = & \quad (\cos\alpha+i\sin\alpha)(\cos\beta+i\sin\beta) \\ = & \quad (\cos\alpha\cos\beta-\sin\alpha\sin\beta)+i(\sin\alpha\cos\beta+\cos\alpha\sin\beta) \end{aligned}$$

Note that this proof also used independence of 1 and $i$. The same argument can be used to find double angle formulas, or triple angle formulas, etc.

The polynomial

$$P(x) = x^n - 1$$

is called a *cyclotomic* polynomial. It's roots are

$$x = e^{2\pi i/n}.$$

If $n = p$ is prime, then

$$P(x) = (x-1)(x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1),$$

and does not factor further.

Let's look more closely at this root

$$x = e^{2\pi i/p} = \cos(2\pi/p) + i\sin(2\pi/p).$$

Its inverse is

$$x^{-1} = e^{-2\pi i/p} = \cos(2\pi/p) - i\sin(2\pi/p).$$

Thus, $w = x + x^{-1}$ is real (in fact, $x^k + x^{-k}$ is real). This number $w$ always satisfies a polynomial of degree $\frac{p-1}{2}$.

For example, let $p = 5$, and $w = x + x^{-1}$. Then

$$w^2 = (x + x^{-1})^2 = x^2 + 2 + x^{-2}$$

and hence

$$\begin{aligned} w^2 + w - 1 &= x^2 + x + 1 + x^{-1} + x^{-2} \\ &= x^{-2}(x^4 + x^3 + x^2 + x + 1) = 0. \end{aligned}$$

Thus, we have just shown that

$$2\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}.$$

**Exercise.** ('62, # 4) Solve the equation

$$\cos^2 x + \cos^2 2x + \cos^2 3x = 1.$$

**Exercise.** ('63, # 5) Prove that

$$\cos(\pi/7) - \cos(2\pi/7) + \cos(3\pi/7) = 1/2$$

## 7. Stereographic projection and Pythagorean triples

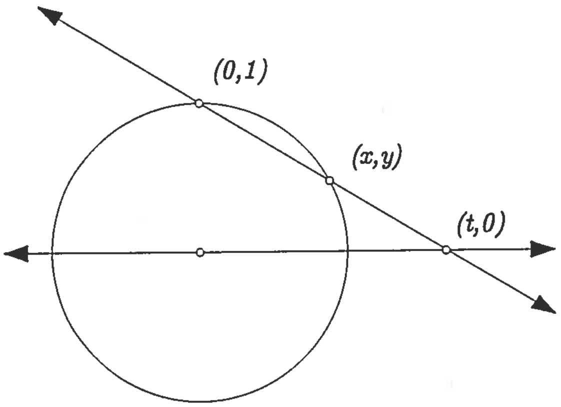
You are probably familiar with Pythagorean triples – integer triples $(a, b, c)$ such that

$$a^2 + b^2 = c^2,$$

such as $(3, 4, 5)$ and $(5, 12, 13)$. You may even be familiar with a general formula for all these triples, and saw this formula derived via a number of algebraic manipulations and repeated observations that certain numbers are squares. In the following, let us take a more geometric approach.

Note that if $(a, b, c)$ is a Pythagorean triple, then $(a/c, b/c)$ is a point on the circle

$$x^2 + y^2 = 1.$$



Let us consider the line through $(0, 1)$ and a point $(t, 0)$ on the $x$-axis. This line intersects the circle at two points – at $(0, 1)$ and (say) at $(x, y)$. Comparing slopes, we get

$$\frac{y-1}{x} = \frac{-1}{t}$$

so

$$x = t(1 - y).$$

Since $(x, y)$ is a point on the circle, this gives

$$\begin{aligned} t^2(y-1)^2 + y^2 - 1 &= 0 \\ (y-1)(t^2(y-1) + (y+1)) &= 0. \end{aligned}$$

The solution $y = 1$ gives the north pole, so we're interested in the other solutions, which are

$$\begin{aligned} y(t^2+1)+(1-t^2) &= 0 \\ y &= \frac{t^2-1}{t^2+1} \\ x &= t\left(1-\frac{t^2-1}{t^2+1}\right) \\ &= \frac{2t}{t^2+1}. \end{aligned}$$

Thus, in terms of $t$, the points on the circle are $\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$. Note that if $t$ is rational, then so are $x$ and $y$, and if $x$ and $y$ are rational, then so it $t$. Now, let us write $t = p/q$. Then

$$(x,y) = \left(\frac{2pq}{p^2+q^2}, \frac{p^2-q^2}{p^2+q^2}\right).$$

If $p > q \geq 0$ are relatively prime, positive, and of different parity, then

$$(a,b,c) = (2pq, p^2-q^2, p^2+q^2).$$

This gives us all Pythagorean triples with $a$ even. Those with $a$ odd are given by the pairs $(p,q)$ both odd, and $(a,b,c) = (pq, (p^2-q^2)/2, (p^2+q^2)/2)$. One can also get those with $a$ odd by finding the solutions with $a$ even and switching $a$ and $b$.

One advantage of this method is that it works for all quadratic curves. For example, try it on $a^2 - 2b^2 = c^2$; on $a^2 + b^2 = 2c^2$; and on $a^2 + b^2 = 3c^2$.

In general, it will not work on cubics, or higher degree curves. (This is a fundamental concept in *algebraic geometry.*) An exception is the curve

$$y^2 = x^3 - x^2.$$

Use stereographic projection on this curve using the point $(0,0)$ and the line $x = 1$.

**Exercise.** ('75, #5) Determine, with proof, whether or not one can find 1975 points on the circumference of a circle with unit radius such that the distance between any two of them is a rational number.

## 8. The prime number theorem

**Theorem 8.1** (The prime number theorem). *Let $\pi(x)$ be the number of primes less than $x$. That is,*

$$\pi(x) = \#\{p \text{ prime} : p < x\}.$$

*Then $\pi(x)$ grows asymptotically like $\dfrac{x}{\log x}$. That is,*

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1.$$

We won't prove this. However, there is a rather clever proof due to Euclid of a weaker version:

**Theorem 8.2.** *There exists an infinite number of primes.*

*Proof.* Suppose there exists only a finite number of primes, say

$$P=\{p_1,p_2,p_3,...,p_n\}=\{2,3,...,p_n\}.$$

Then, consider the number

$$N=p_1p_2\cdots p_n+1.$$

Note that $N$ and $p_i$ are relatively prime for all $i$, so $p_i$ does not divide $N$ for all $p_i$. But since every number factors into a product of primes there exists a prime which divides $N$ and is not in $P$. Thus, $P$ is not complete. Hence there must be an infinite number of primes. □

Note that this also gives us a natural way of ordering the primes. We start with 2. Take the product of all primes we have and add 1 to get $N=3$. The smallest prime divinding $N$ is three, so now we have $\{2,3\}$. We take the product and add 1 to get 7. We now have $\{2,3,7\}$. At the next step, we get 43. We continue indefinitely.

**Exercise.** ('71, # 3) Prove that the set of integers of the form $2^k-3$ for $k=2,3,...$ contains an infinte subset in which every two members are relatively prime.

University of Nevada Las Vegas, Las Vegas, NV 89154-4020
*E-mail address*: baragar@nevada.edu