MATH342 Number Theory

Number theory is about integers. At least, that is the main focus. Other types of numbers come in, and generate studies in their own right, but often the original reason for introducing them was to gain insight into problems about integers.

What questions are asked in number theory?

Questions about prime numbers, in particular, their distribution.

Questions about polynomial equations (usually in several variables) with integer coefficients: are there solutions, and if so, how many.

Examples of questions

Are there infinitely many primes? (Yes!)

Are there infinitely many pairs of consecutive odd integers which are prime? (Unknown! Twin Prime Conjecture)

What integers can be written as the sum of two squares of integers? (Will discuss later)

What numbers can be written as the sum of two positive primes? (Unknown! Goldbach Conjecture)

Review of Basic Material

$\mathbb{Z} = \{0, \pm 1, \pm 2 \cdots\}$ integers

$\mathbb{N} = \{0, 1, 2, 3 \cdots\}$ natural numbers

$\mathbb{Z}_+ = \{1, 2, 3 \cdots\}$ strictly positive integers.

Arithmetic

The sum or product of two integers (or natural numbers, or elements of $\mathbb{Z}_+$) is ~~another~~ an integer (or natural number, or elements of $\mathbb{Z}_+$)

The difference of two integers is an integer.

These arithmetic operations satisfy a number of laws.

Addition and multiplication are both associative:

$$(m+n)+p = m+(n+p) \quad \forall m, n, p \in \mathbb{Z}$$

$$(m.n).p = m.(n.p) \quad \forall m, n, p \in \mathbb{Z}$$

and commutative:

$$m+n = n+m \quad \forall m, n \in \mathbb{Z}$$

$$m.n = n.m \quad \forall m, n \in \mathbb{Z}$$

A <u>distributive</u> law holds:

$$m.(n+p) = (m.n)+(m.p) \quad \forall m, n, p \in \mathbb{Z}$$

There is also an <u>order</u> and modulus

$$m \leq m.n \quad \forall m, n \in \mathbb{Z}_+$$

$$\text{and } m < m.n \quad \forall m \in \mathbb{Z}_+, n \in \mathbb{Z}_+ \text{ with } n \geq 2$$

$$|n| = \pm n \quad \forall n \in \mathbb{Z} \qquad |n| = \begin{cases} +n & \text{if } n \geq 0 \\ -n & \text{if } n < 0 \end{cases}$$

<u>Divisors</u> For $m, n \in \mathbb{Z}$, we say m <u>divides n</u> if

$n = km$ for $k \in \mathbb{Z}$.

This is written $m \mid n$. We also say m is a <u>divisor</u> of n

e.g. $2 \mid 4$ $\quad 2 \nmid 3$ and for all $n \in \mathbb{Z}$:

$$n \mid 0, \quad n \mid \pm n \quad 1 \mid n.$$

We say "$\mathbb{Z}$ has no zero divisors" meaning that if $0 = mn$ for $m, n \in \mathbb{Z}$ then $m = 0$ or $n = 0$.

Primes

$p \in \mathbb{Z}$ is *prime* if $p \neq 0$, $p \neq \pm 1$ and the only divisors of p are $\pm 1, \pm p$.

Examples 2 and 3 are prime. 4 is not.

Euclidean property

$\mathbb{Z}$ is a *Euclidean domain*. It has the *Euclidean property* with *modulus* as the *Euclidean valuation*

$\forall n \in \mathbb{Z}$ and $\forall m \in \mathbb{Z} \setminus \{0\}$ $\exists$ $q, r \in \mathbb{Z}$ with $0 \leq r < |m|$ such that

$$n = qm + r$$

Greatest common divisor

Let $m, n \in \mathbb{Z} \setminus \{0\}$. The *g.c.d* of m and n is the largest $d \in \mathbb{Z}_+$ such that $d | m$ and $d | n$

We can also say that $-d$ is "the" gcd of m and n, or that $\pm d$ is the g.c.d.

Euclidean property has important consequences.

Theorem If $m, n \in \mathbb{Z} \setminus \{0\}$, the gcd of m and n is the smallest ~~integer~~ element of $\mathbb{Z}_+$ of the form $am + bn$ for $a, b \in \mathbb{Z}$.

Proof. Clearly such an integer exists. Call it $d = am + bn$

If $d \nmid m$ then $m = qd + r$ for $1 \leq r < d$

$r = m - q(am + bn) = (1 - qa)m + (-qb)n < d$. $\times$

Corollary Every other divisor of m and n divides $d = am + bn$

Corollary If $\gcd(m,n) = 1$ then $\exists a, b \in \mathbb{Z}$ s.t. $am + bn = 1$

Corollary If $m, p \in \mathbb{Z} \setminus \{0\}$ and $n \in \mathbb{Z}$ and $p \mid mn$ then $p \mid n$

Proof $\gcd(m,p) = 1 \Rightarrow \exists a, b \in \mathbb{Z}$ s.t. $am + bp = 1$

$n = (am + bp)n = a(mn) + (bn)p$ is divisible by p

Corollary p is prime $\Leftrightarrow p \neq 0, \pm 1$ and whenever $p \mid mn$ then $p \mid m$ or $p \mid n$.

Proof $\Leftarrow$ $p = mn \Rightarrow p \mid m$ or $p \mid n \Rightarrow p = \pm m$ and $n = \pm 1$ or $p = \pm n$ or $m = \pm 1$

$\Rightarrow$ $p \mid mn$ and $p \nmid m \Rightarrow \gcd(p,m) = 1 \Rightarrow p \mid n$

Corollary The lowest common multiple l of $m, n \in \mathbb{Z} \setminus \{0\}$ is $\pm \frac{mn}{d}$ where $d = \gcd(m,n)$

Proof $m = dm_1$ and $n = dn_1$ with $\gcd(m_1, n_1) = 1$

Both m and n divide $m_1 n_1 d = \frac{mn}{d}$

Suppose both m and n divide $mn_2 = m_1 d n_2$

$n = n_1 d \mid m_1 d n_2 \Rightarrow n_1 \mid m_1 n_2 \Rightarrow n_1 \mid n_2 \Rightarrow m_1 n_1 d \mid m n_2$

Fundamental Theorem of Arithmetic

Let $n \in \mathbb{Z}_+$, $n \geq 2$. Then $\exists$ k, $\in \mathbb{Z}_+$, primes $p_i \in \mathbb{Z}_+$ $(1 \leq i \leq k)$ and $r_i \in \mathbb{Z}_+$ $(1 \leq i \leq k)$ s.t.

$$n = \prod_{i=1}^{k} p_i^{r_i}$$ k, p_i, r_i are unique given n.

Proof By induction on n. Uniqueness uses: if p is prime and $p | n_1 n_2$ then $p | n_1$ or $p | n_2$.

Examples $135 = 3^3 \times 5$ $136 = 17 \times 2^3$ 137 is prime

Application If $m = \prod_{i=1}^{k} p_i^{r_i}$ and $n = \prod_{i=1}^{k} p_i^{s_i}$ for $r_i, s_i \in \mathbb{N}$ then $\gcd(m,n) = \prod_{i=1}^{k} p_i^{\mathrm{Min}(r_i, s_i)}$

$$\mathrm{lcm}(m,n) = \prod_{i=1}^{k} p_i^{\mathrm{Max}(r_i, s_i)}$$

Application If $n \in \mathbb{Z}_+$ is not of the form k^2 $(k \in \mathbb{Z}_+)$ then there do not exist $a, b \in \mathbb{Z}_+$ s.t.

$$a^2 = n b^2$$

Proof $a^2 = \prod_{i=1}^{k} p_i^{2r_i}$ & $b^2 = \prod_{i=1}^{l} q_i^{2s_i}$

$$\prod_{i=1}^{k} p_i^{2r_i} = n \prod_{i=1}^{l} q_i^{2s_i} \implies n \text{ must be a product of}$$

even powers of primes $\times$.

<u>Application</u> If $n = \prod_{i=1}^{k} p_i^{r_i}$ for distinct primes p_i then the number of divisors of n is

$$\prod_{i=1}^{k} (r_i + 1)$$

<u>Example</u> $135 = 3^3 \times 5$. So the number of divisors is $4 \times 2 = 8$

<u>Solving linear equations over $\mathbb{Z}$</u>

If $a \neq 0$ and $a, b \in \mathbb{Z}$ then
$ax = b$ has a solution $x \in \mathbb{Z} \Leftrightarrow a \mid b$ and
then the solution is unique

If $a, b, c \in \mathbb{Z}$ and $a \neq 0$, $b \neq 0$, the equation
$ax + by = c$ has solutions $x \in \mathbb{Z}$ $y \in \mathbb{Z}$
$\Leftrightarrow \gcd(a, b) \mid c$

If $c = kg$ then $\exists x_0, y_0 \in \mathbb{Z}$ s.t.

$ax_0 + by_0 = g$

$x_1 = kx_0$, $y_1 = ky_0$ is one solution

$ax + by = c \Leftrightarrow a(x - x_1) + b(y - y_1) = 0$

$\Leftrightarrow a_1(x - x_1) + b_1(y - y_1) = 0$ where $a = a_1 g$, $b = b_1 g$

If this holds then $\gcd(a_1, b_1) = 1 \Rightarrow b_1 \mid x - x_1$

and $a_1 \mid y - y_1$

So $x - x_1 = n b_1$ and $y - y_1 = -n a_1$ for some $n \in \mathbb{Z}$

So $x = k x_0 + n b_1$, $y = k y_0 - n a_1$ for $n \in \mathbb{Z}$

is the general solution.

Solutions in $\mathbb{N}$

Which numbers in $\mathbb{N}$ can be written in the form

$2a + 3b$ for $a, b \in \mathbb{N}$?

$0, 2, 3$, any number ≥ 4 e.g. $2k$ (for even numbers)

$3 + 2k$ (for odd numbers ≥ 3)

$2a + 5b$ for $a, b \in \mathbb{N}$?

$0, 2, 4, 5, 6$, any number ≥ 4

$3a + 9b$ for $a, b \in \mathbb{N}$?

All numbers divisible by 3.

What about $5a + 11b$ for $a, b \in \mathbb{N}$?

Various numbers between 0 and 40 and then all integers

≥ 40

Why? More generally, let $p, q \in \mathbb{Z}_+$, $\gcd(p,q) = 1$.

Let $p < q$. All integers $\geq pq - q$ can be written as $ap + bq$ for $a, b \in \mathbb{N}$

To see this: given n, we can find $a_1, b_1 \in \mathbb{Z}$ s.t.

$$a_1 p + b_1 q = n \quad (\text{since } \gcd(p,q) = 1)$$

$$(a_1 + kq)p + (b_1 - kp)q = n \quad \forall k \in \mathbb{Z}$$

We can choose $k \in \mathbb{Z}$ so that

$$0 \leq b_1 - kp \leq p - 1$$

If $n \geq pq - q$ then $a_1 + kq \geq 0$

<u>The Euclidean algorithm</u> is a method for finding the gcd of $m, n \in \mathbb{Z} \setminus \{0\}$

Might as well take $m, n \in \mathbb{Z}_+$, $n > m$

$$n = q_1 m + r_1 \qquad q_1, r_1 \in \mathbb{N},\ 0 \leq r_1 < m$$

$$m = q_2 r_1 + r_2 \qquad \text{If } r_1 = 0 \text{ then stop}$$

$$\vdots$$

$$r_{k-2} = q_k r_{k-1} + 0 \qquad n > m > r_1 \cdots > r_{k-1} > r_k = 0$$

$$r_{k-1} = \gcd(m,n) \qquad r_0 = m$$

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} q_{i+1} r_i + r_{i+1} \\ r_i \end{pmatrix} = \begin{pmatrix} q_{i+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i-1} - q_{i+1} r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$

So
$$\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = \begin{pmatrix} n_1 r_{k-1} \\ m_1 r_{k-1} \end{pmatrix}$$

$$\begin{pmatrix} r_{k-1} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix}$$

$$ab' - a'b = (-1)^k \qquad \text{So } \gcd(a,b) = \gcd(a',b') = 1$$

$$r_{k-1} = an + bm \qquad \text{lcm} = \pm a'n = \pm b'm$$

Examples

① $\left(\begin{array}{cc|c} 1 & 0 & 255 \\ 0 & 1 & 135 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 120 \\ 0 & 1 & 135 \end{array}\right) \xrightarrow[R_2 - R_1]{} \left(\begin{array}{cc|c} 1 & -1 & 120 \\ -1 & 2 & 15 \end{array}\right)$

$\xrightarrow{R_1 - 8R_2} \left(\begin{array}{cc|c} 9 & -17 & 0 \\ -1 & 2 & 15 \end{array}\right)$ $\quad \gcd(255, 135) = 15$

$-255 + 2 \times 135 = 15 \qquad lcm = 9 \times 255 = 17 \times 135$

② $\left(\begin{array}{cc|c} 1 & 0 & 255 \\ 0 & 1 & 136 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 119 \\ 0 & 1 & 136 \end{array}\right) \xrightarrow[R_2 - R_1]{} \left(\begin{array}{cc|c} 1 & -1 & 119 \\ -1 & 2 & 17 \end{array}\right)$

$\xrightarrow{R_1 - 7R_2} \left(\begin{array}{cc|c} 8 & -15 & 0 \\ -1 & 2 & 17 \end{array}\right)$ $\quad \gcd(255, 136) = 17$

$-255 + 2 \times 136 = 17$

$8 \times 255 = 15 \times 136 = lcm$

③ $\left(\begin{array}{cc|c} 1 & 0 & 255 \\ 0 & 1 & 137 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 1 & -1 & 118 \\ 0 & 1 & 137 \end{array}\right) \xrightarrow[R_2 - 2R_1]{} \left(\begin{array}{cc|c} 1 & -1 & 118 \\ -1 & 2 & 19 \end{array}\right)$

$\xrightarrow{R_2 - 118R_1} \cancel{\left(\begin{array}{cc|c} 255 & -137 & 0 \\ -1 & 2 & 1 \end{array}\right)}$ $\quad \gcd \cancel{(255, 137) = 1}$

$-\cancel{255} + 2\times$

$\xrightarrow{R_1 - 6R_2} \left(\begin{array}{cc|c} 7 & -13 & 4 \\ -1 & 2 & 19 \end{array}\right) \xrightarrow[R_1 - 4R_2]{} \left(\begin{array}{cc} 7 & -13 \\ -29 & 54 \end{array}\right) \xrightarrow{R_1 - R_2} \left(\begin{array}{cc|c} 36 & -67 & 1 \\ -29 & 54 & 3 \end{array}\right)$

$\xrightarrow[R_2 - 3R_1]{} \left(\begin{array}{cc|c} 36 & -67 & 1 \\ -137 & 255 & 0 \end{array}\right)$ $\quad \gcd(255, 137) = 1$

Modulo arithmetic

For $p \in \mathbb{Z} \setminus \{0\}$ ~~we write~~ and $n_1, n_2 \in \mathbb{Z}$, we write

$n_1 \equiv n_2 \bmod p$ if $p \mid n_1 - n_2$ – omitting mod p if it is clear from the context.

$\equiv \bmod p$ is an equivalence relation, called <u>congruence mod p</u>

$n_1 \equiv n_2 \bmod p \iff n_2 = n_1 + kp$ for some $k \in \mathbb{Z}$.

If $n_1 \equiv n_2 \bmod p$ and $m_1 \equiv m_2 \bmod p$ then $n_1 + m_1 \equiv n_2 + m_2 \bmod p$

and $n_1 m_1 \equiv n_2 m_2 \bmod p$

because $n_2 = n_1 + kp$ and $m_2 = m_1 + lp \Rightarrow n_2 m_2 = n_1 m_1 + p(k + l + kl)$

<u>Examples</u> $1 + 1 \equiv 0 \bmod 2$

$2 \times 2 \equiv 1 \bmod 3$

$x - 1 \equiv 0 \bmod 3 \iff x \equiv 1 \bmod 3$

$x + 1 \equiv 0 \bmod 3 \iff x \equiv -1 \bmod 3 \iff x \equiv 2 \bmod 3$

$x \equiv 1 \bmod 3 \iff 2x \equiv 2 \bmod 3$

because $2x \equiv 2 \bmod 3 \implies 2 \times 2x \equiv 2 \times 2 \bmod 3$

$\implies x \equiv 1 \bmod 3$

For any $p \in \mathbb{Z}_+$, $p \geq 2$, $\{n \bmod p : n \in \mathbb{Z}\}$ is a <u>commutative ring with identity</u>. The identity element is $1 \bmod p$.

The arithmetic operations are addition and multiplication mod p.

$r \bmod p$ ~~$r \in \mathbb{Z}$~~ has a (multiplicative) inverse mod p ~~iff~~ $\iff$

$r \neq 0$ and $\gcd(p, r) = 1$

A multiplicative inverse ~~of~~ of $r \bmod p$ is $s \bmod p$ s.t.

$rs = 1 \bmod p$.

$rs = 1 \bmod p \iff rs + ap = 1$ for some $a \in \mathbb{Z}$.

So s exists $\iff \gcd(r, p) = 1$.

If $rs_1 \equiv rs_2 \equiv 1 \bmod p$ then $s_1 \equiv s_2 \bmod p$

because $s_1 \equiv s_1 r s_2 \equiv (rs_1) s_2 \equiv s_2 \bmod p$.

If $p \in \mathbb{Z}_+$ is prime then $r \bmod p$ has an inverse

mod p $\forall\ 1 \leq r \leq p-1$.

<u>Examples</u> $2^{-1} \equiv 2 \bmod 3$ because $2 \times 2 \equiv 1 \bmod 3$

$2^{-1} \equiv 3 \bmod 5$ $\quad 4^{-1} \equiv 4 \bmod 5$

<u>Example</u> $3 \mid 2^n - 1 \iff n$ is even, for $n \in \mathbb{N}$

To see this: $2^2 \equiv 1 \bmod 3$. $\quad 2^0 = 1 \equiv 1 \bmod 3$

So $2^{2k} = (2^2)^k = 1^k = 1 \bmod 3 \quad \forall k \in \mathbb{Z}_+$

$2^{2k+1} \equiv 2^{2k} \times 2 \equiv 1 \times 2 \equiv 2 \bmod 3$ for all $k \in \mathbb{Z}$.

$2^{2k} - 1 \equiv 0 \bmod 3 \qquad 2^{2k+1} - 1 \equiv 1 \bmod 3$.

Of course there are other ways of doing this

For any x

$$x^{2k}-1 = (x^2-1)(1+\dots+x^{2(k-1)})$$

Putting $x=2$, $2^{2k}-1 = (2^2-1)(1+\dots+2^{2(k-1)})$

$$= 3\times(1+\dots+2^{2(k-1)})$$

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

Putting $x=2$, $2^{2k+1}-1 = 2(2^{2k}-1)+1$

<u>Example</u> How many solutions to $x^2 \equiv 1 \bmod 3$?

Check $x\equiv 0$, $x\equiv 1$, $x \equiv 2$

$x\equiv 1 \bmod 3$ and $x\equiv 2 \bmod 3$ are both solutions.

<u>Example</u> How many solutions to $x^3 \equiv 1 \bmod 7$?

Check $x\equiv 0, 1, 2, 3, 4., 5, 6$

$0^3\equiv 0$, $1^3 \equiv 1$ $2^2\equiv 4 \equiv$, $2^3\equiv +1$

$3^2\equiv +2$, $3^3\equiv -1$ $4^3\equiv(-3)^3\equiv +1$ $5^3\equiv(-2)^3\equiv -1$

$6^3\equiv(-1)^3\equiv -1$

~~$x\equiv 1$ is the only solution.~~

However $x^3\equiv 1 \bmod 5$ has only one solution.