Midterm 1 Friday July 8th Gradescope (2 hrs within 24 hrs)
take home
5-6 problems
2 + 3 (w1, w2) Induction, Sets

Introduction to Number Theory

Number theory is a study of integers $\mathbb{Z} = \{ \dots -3, -2, -1, 0, 1, 2, 3, \dots \}$

Many problems are about prime numbers.

Def: We say that $a \mid b$ "a divides b" for $a, b \in \mathbb{Z}$ if $\exists c \in \mathbb{Z}$ s.t. $b = a \cdot c$ (or b is divisible by a)

Ex: $6 \mid 18$ $\quad 18 = 6 \cdot 3$

$10 \mid 10$ $\quad 10 = 10 \cdot 1$

$7 \mid 0$ $\quad 0 = 7 \cdot 0$ $\leftarrow$ every integer divides zero

$3 \nmid 5$ $\qquad a \nmid b$ if $\nexists\, c \in \mathbb{Z}$ s.t. $b = a \cdot c$

Properties of divisibility:

- if $a \mid b$ and $b \mid c \Rightarrow a \mid c$

Proof: $\exists d: b = a \cdot d \qquad \exists e: c = b \cdot e = a \underbrace{(d \cdot e)}_{\in \mathbb{Z}}$

- $a \mid b \Rightarrow a^{1000} \mid b^{1000}$ $\quad (a^n \mid b^n)$ $n \in \mathbb{Z}$

Proof: $\exists c \in \mathbb{Z}$ s.t. $b = a \cdot c$

$b^n = (a \cdot c)^n = (a^n)\underbrace{(c^n)}_{\in \mathbb{Z}}$

- if $a \mid x$, $a \mid y \Rightarrow a \mid mx + ny$ $\quad \forall m, n \in \mathbb{Z}$

Proof: $\exists c, d \in \mathbb{Z}$ s.t.

$x = a \cdot c$, $y = a \cdot d$

$mx + ny = m \cdot a \cdot c + n \cdot a \cdot d = a \underbrace{(mc + nd)}_{\in \mathbb{Z}}$

$\Rightarrow a \mid mx + ny$

Ex: $6 \mid 36$, $6 \mid 12 \Rightarrow 6 \mid 96$

$96 = \underbrace{1}_{n} \cdot 36 + \underbrace{5}_{m} \cdot 12$

Def: An even number x is s.t. $2 \mid x$

An odd number x is s.t. $2 \nmid x$

Theorem (Euclid's division Algorithm)

If $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ s.t.

$$a = b \cdot \underbrace{q}_{\text{quotient}} + \underbrace{r}_{\text{remainder}}$$

Ex: $a = 100$, $b = 3$

$$100 = 3 \cdot \underbrace{33}_{q} + \underbrace{1}_{r}$$

Idea: try different values of q until $100 - 33 \cdot q$ becomes negative

$\Rightarrow$ too far

Proof: First find q, r, then prove uniqueness

Let $S = \{ a + b \cdot y \mid y \in \mathbb{Z} \}$

$S^+ \subset S$ – all non-negative elements of S

r – smallest element in S^+

$a = 100$, $b = 3$

$S = \{ \ldots, -2, 1, 4, 7, 10 \ldots \ldots 94, 97, 100, 103, 106, \ldots \}$

$S^+ = \{ 1, 4, 7, 10, \ldots \}$

$\downarrow$ r

Claim: $0 \le r < b$ since $r \in S \Rightarrow r = a + b \cdot y$ for some $y \in \mathbb{Z}$

$r \ge 0$ since $r \in S^+$

Suppose $r \ge b \Rightarrow r' = r - b = a + b \cdot y - b = a + b\underbrace{(y-1)}_{\mathbb{Z}} \ge 0$

$\Rightarrow r' \in S^+$

Contradiction because r is the smallest element in S^+

$\Rightarrow r < b$

$$r = a + b \cdot y \Rightarrow a = r + b\underbrace{(-y)}_{q}$$

Now prove uniqueness: Assume not unique $\exists\ r', q' \in \mathbb{Z}$ s.t.

$a = b \cdot q + r \qquad 0 \le r < b$

$- \quad a = b\, q' + r' \qquad 0 \le r' < b$

$0 = a - a = b(q - q') + (r - r')$

$b(q - q') = r' - r \Rightarrow b \mid r' - r$

$|r' - r| < b \quad \Rightarrow r' = r$

$q = q'$

Ex: Show that $5 \mid n^5 - n \quad \forall n \in \mathbb{Z}_+$

1) $n=1 \quad n^5 - n = 0 \quad 5 \mid 0$ ← base of induction

$n=2 \quad n^5 - n = 30 \quad 5 \mid 30$

2) Inductive assumption: for some n $\quad 5 \mid n^5 - n$

3) Inductive step: $(n+1)^5 - (n+1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + \cancel{1} - n - \cancel{1}$

$$
\begin{array}{cccccc}
 & & 1 & & & \\
 & 1 & & 1 & & \\
1 & & 2 & & 1 & \\
1 & 3 & & 3 & 1 & \\
1 & 4 & 6 & 4 & 1 & \\
1 & 5 & 10 & 10 & 5 & 1
\end{array}
$$

$= \underbrace{n^5 - n}_{\text{divisible by } 5} + 5(\underbrace{n^4 + 2n^3 + 2n^2 + n}_{\in \mathbb{Z}})$ $= 5 \cdot d$

$n^5 - n = 5 \cdot C$

$5 \mid n^5 - n$

5 divides this number

$= 5 \mid (n+1)^5 - (n+1)$

$5(C+d)$

Prime numbers

Def: A number $p \in \mathbb{Z}$ is prime is $p > 0$ and has exactly two divisors: 1 and p.

$2, 3, 5, 7, 11, 13, 17, 19, \ldots$

The largest known prime: $2^{74,207,281} - 1 \sim 10^{20,000,000}$

$$\log_b a = \frac{\log a}{\log b}$$

$$\log_{10} 2 = \frac{\log 2}{\log 10} \approx 0.301\ldots$$

$2^{10} = 10^{\overbrace{10 \cdot \log 2}^{3}} \sim 10^3$

$2^{100} \sim 10^{30}$

$\pi(x) = \#$ primes $< x$

$\pi(10) = 4$

$\pi(20) = 8$ ←

$x = 20$

$\dfrac{20}{\log 20} \approx 6.7$

$$\pi(x) \approx \frac{x}{\log x}$$

Theorem: There are infinitely many primes

idea: $a \mid b, \; a > 1$

$\quad a \nmid b+1$

$6 \mid 12 \qquad 7 \mid 21$

$6 \nmid 13 \qquad 7 \nmid 22$

$\exists c \in \mathbb{Z}$ s.t. $b = a \cdot c$

assume $a \mid b+1 \Rightarrow \exists d \in \mathbb{Z}$ s.t. $b+1 = a \cdot d$

$a \cdot c + 1 = a \cdot d$

$1 = a(d-c) \Rightarrow a \mid 1$

$\Rightarrow a = 1$

$100 = \underset{c}{5} \cdot \underset{a}{20}$ (with $b = 100$)

$101 \neq 6 \cdot 20$

$120 = 6 \cdot 20$

	20	40	60	80	100	120
c	1	2	3	4	5	6

Proof: Assume there are finitely many primes

$\{p_1, p_2, \dots, p_k\}$ - complete list of all primes.

$N = p_1 \cdot p_2 \cdot \dots \cdot p_k$ by construction $p_i \mid N$, $i = 1, \dots, k$

but $p_i \nmid N+1$, $i = 1, \dots, k$

Does $N+1$ have any divisors?

Yes: • $1, N+1$ and no other divisors $\Rightarrow N+1$ is prime

• $N+1 = a \cdot b$, $a, b < N+1$

$a \mid N+1$

How about a?

If a has a and 1 as its only divisors $\Rightarrow a$ prime

o/w $a = c \cdot d$, $c, d < a$

How about c?

⋮

the process terminates when we find a prime p s.t. $p \mid N+1$

$p \neq p_1, p_2, \dots p_k$

$\Rightarrow$ contradiction so set of primes is infinite.

Finding primes **Sieve of Eratosthenes**

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

do over (2 → smallest non-crossed number)

- cross out all multiples of 2 except 2
- circle the first non crossed number

Ex: run the loop 3 times $\quad \pi(30)=10$

Q: Given $N\in\mathbb{Z}$ how many times do you need to run the algorithm?

A: $\sqrt{N}$

$K>N$

$K\le N$

If $a>\sqrt{N}$, pick $K<N$ $\quad$ a) $K \Rightarrow K=a\cdot c$ $\quad (c|K)$

$K\sim N$ $\quad c<\sqrt{N}$

Find the largest a s.t. $a^2\le N$

Pick $K<N$: $K=a\cdot c$ $\quad c<\sqrt{N}$

c has already been crossed out

$$\underbrace{2,3}_{1},\underbrace{\ ,5}_{2},\underbrace{\ ,7}_{2},\underbrace{\ ,11}_{4},\underbrace{\ ,13}_{2},\underbrace{\ ,17}_{4},\underbrace{\ ,19}_{2},\underbrace{\ ,23}_{4},\underbrace{\ ,29}_{6},\underbrace{\ ,31}_{2}$$

$4K+1:\quad 5,\ 13,\ 17,\ 29\ \ldots \quad \equiv 1 \pmod 4$ $\quad$ congruent to

$13\equiv 1 \pmod 4$

$4K+3:\quad 3,\ 7,\ 19,\ 23\ \ldots \quad \equiv 3 \pmod 4$

Proposition: Given any N there are two consecutive primes which are $\geq N$ apart from each other,

$$\ldots\ \underbrace{P_K\ \ldots\ \ldots\ P_{K+1}}_{\geq N},\ \ldots \iff P_{K+1}-P_K\geq N$$

no primes

$$\Gamma(z)=\int_0^\infty e^{-t}t^{z-1}\,dt$$

Stirling approximation:

$$n!\approx\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\ldots$$

Proof: $\quad n!=1\cdot2\cdot3\cdot4\cdot\ldots\cdot(n-1)\cdot n$

$$\begin{cases} a_1=(n+1)!+2\\ a_2=(n+1)!+3\\ \vdots\\ a_i=(n+1)!+i+1\\ \vdots\\ a_n=(n+1)!+n+1\end{cases}$$

$n=10$

$a_1=11!+2=481,466,702$

$a_2=11!+3=481,466,703$

$\vdots$

$\sim e^{(n-\frac12)\log n}$

$\sim e^{24}$

$\sim 10^9$

$(i+1)\mid a_i$ since $(n+1)!=1\cdot2\cdot3\cdot4\cdot\ldots\cdot(i+1)\cdot\ldots\cdot n\cdot(n+1)$

$a_i = (i+1)\left(\frac{(N+1)!}{i+1}+1\right)$, so all a_i are composite

$$n = N-1$$

The Fundamental theorem of Arithmetic (FTA)

For any integer $N>1$ there is a prime factorization of N:

There are distinct primes $p_1, p_2 \dots p_k$, and $\underbrace{r_1,\dots,r_k}_{\text{multiplicities}}$, $r_k \geq 1$, $r_k \in \mathbb{Z}$ s.t.

$$N = p_1^{r_1} \cdot p_2^{r_2} \cdot p_3^{r_3} \cdot \ldots \cdot p_k^{r_k}$$

This factorization is unique up to reordering.

$16 = 2^4$ $\quad p_1 = 2,\ r_1 = 4$

$40 = 2^3 \cdot 5$ $\quad p_1 = 2,\ r_1 = 3$
$\quad p_2 = 5,\ r_2 = 1$

Ex: $\mathbb{Z}$ - ring $\qquad \mathbb{C} = \mathbb{R}[\sqrt{-1}]$ $\qquad i^2 = -1$

$x^2 + 5 = 0$

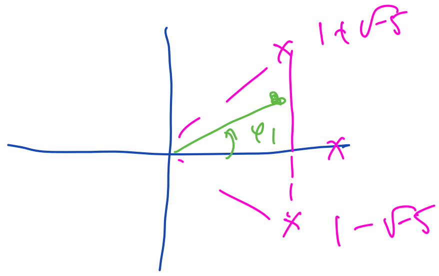
Gaussian numbers
ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\,b \mid a, b \in \mathbb{Z}\} \supset \mathbb{Z}$$

$\mathbb{Z}$ adjoin element $\sqrt{-5}$

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

$\Rightarrow$ Gaussian prime decomposition is not unique!



$z_1 = |z_1| \cdot e^{i\varphi_1}$

$z_1 \cdot z_2$

$= |z_1||z_2| \cdot e^{i\varphi_1 + i\varphi_2}$

Def: Let $a, b \in \mathbb{Z}$ not both equal to zero. The greatest common divisor of a and b $\quad \gcd(a,b) = (a,b) = d$

is the largest integer that divides a and b.

Ex: $\gcd(6, 15) = 3$ $\qquad \gcd(100, 76) = 2^2 = 4$

$6 = 2 \cdot 3$, $15 = 3 \cdot 5$ $\qquad 100 = 2^2 \cdot 5^2$, $76 = 2^2 \cdot 19$

$\gcd(105, 0) = 105$ $\qquad \gcd(2022{,}2022{,}2022,\ 2022{,}2022) = ?$

Division algorithm

Idea: $a, b \in \mathbb{Z}$ $\quad a = b\cdot q + r$, $0 \le r < b$

$\gcd(a,b)$ $\quad \gcd(b,r)$

Ex:

$\gcd(\underset{2\cdot 3^2 7}{126}, \underset{3^3}{27}) = 3^2 = 9$

$126 = 27\cdot 4 + 18$

$\gcd(\underset{3^3}{27}, \underset{2\cdot 3^2}{18}) = 9$

Ex:

$a = 502$, $b = 98$

$502 = b\cdot 5 + 12$

$\gcd(\underset{2\cdot 251}{502}, \underset{2\cdot 7^2}{98}) = 2$

$\gcd(\underset{2\cdot 7^2}{98}, \underset{2^2\cdot 3}{12}) = 2$

Lemma: Let $a, b \in \mathbb{Z}$, $a, b \neq 0$. Then $\overset{A}{\gcd(a,b)} = \overset{B}{\gcd(b,r)}$ where $r = a - b\cdot q$ for some $q \in \mathbb{Z}$, $0 \le r < b$.

Proof: $\{A = B\} \iff \{A \ge B\} \wedge \{B \ge A\}$.

($\ge$) Let $c \in \mathbb{Z}$, $c \mid a$, $c \mid b$ $\Rightarrow c \mid \underbrace{(a\cdot 1 + b\cdot(-q))}$, $q \in \mathbb{Z}$ (quotient)

$\Rightarrow c \mid r$

$\Rightarrow \gcd(a,b) \mid r$

So $\gcd(b,r) \ge \gcd(a,b)$

($\le$) Let $d \in \mathbb{Z}$, $d \mid b$, $d \mid r$ $\Rightarrow d \mid \underbrace{(b\cdot q + r)}_{a} = d \mid a$

$\Rightarrow \gcd(b,r) \mid a$

So $\gcd(a,b) \ge \gcd(b,r)$

Therefore $\gcd(b,r) = \gcd(a,b)$.

Algorithm of computing of $\gcd(a,b)$ (Euclid)

- $a = b\cdot q_1 + r_1$ $\quad 0 \le r_1 < b$
- $b = r_1\cdot q_2 + r_2$ $\quad 0 \le r_2 < r_1$
- $r_1 = r_2\cdot q_3 + r_3$ $\quad 0 \le r_3 < r_2$

$\vdots$

Lemma

$\gcd(a,b) = \gcd(b, r_1)$

$\gcd(b, r_1) = \gcd(r_1, r_2)$

$\gcd(r_1, r_2) = \gcd(r_2, r_3)$

$\vdots$

- $r_{k-3} = r_{k-2} \cdot q_{k-1} + \boxed{r_{k-1}}$ $\quad 0 \le r_{k-1} < r_{k-2}$ $\quad \gcd(r_{k-3}, r_{k-2}) = \gcd(r_{k-2}, r_{k-1})$
- $r_{k-2} = r_{k-1} \cdot q_k + \underbrace{\boxed{r_k}}_{=0}$ $\quad \gcd(r_{k-2}, r_{k-1}) = \gcd(r_{k-1}, 0) = r_{k-1}$

$$r_{k-1} = \gcd(a,b)$$

Ex: $\gcd(\overset{a}{12}, \overset{b}{10}) = 2$

$\overset{a}{12} = \overset{b}{10} \cdot \overset{q_1}{1} + \overset{r_1}{\boxed{2}}$

$\underset{q_1}{10} = \underset{r_1}{2} \cdot \underset{q_2}{5} + \underset{r_2}{0}$

Ex: $\gcd(60, 37) = 1$

$60 = 37 \cdot 1 + 23$

$37 = 23 \cdot 1 + 14$

$23 = 14 \cdot 1 + 9$

$14 = 9 \cdot 1 + 5$

$9 = 5 \cdot 1 + 4$

$5 = 4 \cdot 1 + \boxed{1}$

$4 = 4 \cdot 1 + 0$

Ex: $\gcd(2022\,2022\,2022, 2022\,2022) = 2022$

$2022\,2022\,2022 = 2022\,2022 \cdot 10000 + \boxed{2022}$

$2022\,2022 = 2022 \cdot 10000 + 2022$

$= 2022 \cdot 10001 + 0$

Ex: $a = b \cdot q + r \quad a \geq b$

$\gcd(27, 15) = 3$

1) $27 = 15 \cdot 1 + 12$

$15 = 12 \cdot 1 + \boxed{3}$

$12 = 3 \cdot 4 + 0$

2) $15 = 27 \cdot 0 + 15$

$27 = 15 \cdot 1 + 12$

$15 = 12 \cdot 1 + \boxed{3}$

$12 = 3 \cdot 4 + 0$

Theorem: Let $a, b \in \mathbb{Z}$, not both equal to zero.

Then $\gcd(a,b) = \min\{Xa + Yb \mid X, Y \in \mathbb{Z},\ Xa + Yb > 0\}$

smallest number in set

Ex: $\gcd(701, 33) = 701 \cdot X + 33 \cdot Y = 1$

Euclid: $701 = 33 \cdot 21 + 8$

$33 = 8 \cdot 4 + \boxed{1}$

$8 = 1 \cdot 8 + 0$

$1 = 33 - 8 \cdot 4 = 33 - (701 - 33 \cdot 21) \cdot 4$

$$= 33 - 701\cdot 4 + 33\cdot 84$$

$$= \underbrace{701\cdot(-4)}_{X} + 33\cdot \underbrace{85}_{Y}$$

Ex:

$\gcd(60,37)$

6 $\quad 60 = 37\cdot 1 + 23$

5 $\quad 37 = 23\cdot 1 + 14$

4 $\quad 23 = 14\cdot 1 + 9$

3 $\quad 14 = 9\cdot 1 + 5$

2 $\quad 9 = 5\cdot 1 + 4$

1 $\quad 5 = 4\cdot 1 + \boxed{1}$

$$1 = 5 - 4 = 5 - (9-5)$$

$$= 5\cdot 2 - 9$$

$$\overset{3}{=} (14-9)\cdot 2 - 9 = 14\cdot 2 - 9\cdot 3$$

$$\overset{4}{=} 14\cdot 2 - (23-14)\cdot 3 = 14\cdot 5 - 23\cdot 3$$

$$\overset{5}{=} (37-23)\cdot 5 - 23\cdot 3 = 37\cdot 5 - 23\cdot 8$$

$$\overset{6}{=} 37\cdot 5 - (60-37)\cdot 8$$

$$= 37\cdot \underbrace{13}_{Y} + 60\underbrace{(-8)}_{X}$$

Theorem: Let $a, b \in \mathbb{Z}$, not both equal to zero.

Then $\gcd(a,b) = \min\{Xa + Yb \mid X, Y \in \mathbb{Z},\ Xa + Yb > 0\}$

smallest number in set

Proof: $S = \{Xa + Yb \mid X, Y \in \mathbb{Z}\}$

$S^+ = \{$ positive elements of $S\}$

1) Show that the minimum divides a and b

Let $ma + nb$ be the smallest element of S^+

Decision algorithm $\quad a = (ma+nb)\cdot q + r, \quad 0 \le r < ma+nb$

$$r = a - (ma+nb)q = a\underbrace{(1-mq)}_{X} + b\underbrace{(-nq)}_{Y}$$

if $r \neq 0$ then $r = aX + bY \in S^+$

but $r < ma+nb$, contradiction

since $ma+nb$ is the smallest element in S^+

which means $r = 0$. So $ma+nb \mid a$

Analogously, $ma+nb \mid b$ (Exercise)

2) Show that $ma + nb = \gcd(a, b)$

Since $\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$ $\Rightarrow$ $\gcd(a,b) \mid ma+nb$

$\gcd(a,b) \leq ma+nb$

According to step 1) $ma+nb \mid a$, $ma+nb \mid b$ $\Rightarrow$ $ma+nb \leq \gcd(a,b)$

$\Downarrow$

$\gcd(a,b) = ma+nb.$