1 Common functions

- τ is the number of positive divisors of a function. A prime p is $\tau(p) = 2$.
- σ is the sum of positive divisors of a function. A prime p is $\sigma = p + 1$.
- π is the number of primes $\leq n$. A prime p is $\pi(p) = \pi(p-1) + 1$.
- The sum of an arithmetic series can be given by $(\frac{(a_n - a_0)}{\Delta x} + 1) \cdot \frac{(a_n + a_0)}{2}$.
- The sum of a geometric series can be given by $\frac{a_{n+1} - a_0}{r - 1}$.

2 Integers

2.1 Prime sum of squares

If $a^2 + b^2 = c$ is prime, then $c = 1 \pmod 4$.

2.2 Sum of squares

For any sum of squares $a^2 = b^2 + c^2$, $2a^2 = (b+c)^2 + (b-c)^2$. Similarly, $\frac{a^2}{2} = (\frac{b+c}{2})^2 + (\frac{b-c}{2})^2$.

2.3 Odd σ

$\sigma(n)$ is odd if and only if n is of the form $n = 2^k \cdot \ell^2$.

2.4 Calculating τ

It is a matter of adding one to each prime factor and multiplying these terms by each other. $40 = 2^3 \cdot 5 = (3+1)(1+1) = 8$

2.5 Calculating σ

$120 = 2^3 \cdot 3 \cdot 5$. $\sigma(120) = (1 + 2 + 2^2 + 2^3)(1+3)(1+5)$

2.6 Divisibility criteria

Draw lines with the tens place on the x and and the ones place on the y. Try to find a line with an $m \leq |1|$. Use this line to determine divisibility. You can't use it to find remainders.

2.7 Square numbers

"Brahmagupta-Diophantus identity": $(ax + by)^2 + (ay - bx) = (a^2 + b^2) \cdot (x^2 + y^2)$

I'm not sure if this is right

3 Continued fraction decomposition

For a fraction, the cfrac can be calculated by subtracting the integer part, flipping the fractional part, and doing this until you end up with an integer.

Example:

$$\frac{39}{17} = 2 + \frac{5}{17}$$
$$\frac{17}{5} = 3 + \frac{2}{5}$$
$$\frac{5}{2} = 2 + \frac{1}{2}$$

Then the cfrac is

$$2 + \frac{1}{3 + \frac{1}{2 + \frac{1}{2}}}$$

3.1 Continued fractions of square roots

For a $\sqrt{n}$, start by generating all the perfect squares $\leq n$. This will make our job easier. We do this because we can solve for positive integers using the difference of squares, $a^2 - b^2 = (a+b)(a-b)$.

For $\sqrt{23}$, we have

$$(\sqrt{23}+4)(\sqrt{23}-4) = 23 - 16 = 7$$
$$(\sqrt{23}+3)(\sqrt{23}-3) = 14$$
$$(\sqrt{23}+2)(\sqrt{23}-2) = 19$$
$$(\sqrt{23}+1)(\sqrt{23}-1) = 22$$

We will be able to similarly let

$$\sqrt{23} = 4 + (\sqrt{23} - 4)$$

where

$$\sqrt{23} - 4 = \frac{7}{\sqrt{23}+4}$$

Flipping

$$\sqrt{23} = 4 + \frac{7}{\sqrt{23}+4}$$
$$\frac{\sqrt{23}+4}{7} = 1 + \frac{\sqrt{23}-3}{7}$$

and for each fractional part, you rationalize the denominator, like

$$\frac{\sqrt{23}-3}{7} \cdot \frac{\sqrt{23}+3}{\sqrt{23}+3} = \frac{2}{\sqrt{23}+3}$$

until the end.

4 Diophantine equations

Tips:

- From the book: if $ax = ab \pmod p$, then we can rewrite as $x = b \pmod p$. Then for any $ax = b \pmod p$, we can just add $ax = (b + kp) \pmod p$ until we can cancel a common factor from both sides.

4.1 Greatest k in positive integers

For a linear diophantine equation of the form $ax + by = k$, where all variables are positive integers, the greatest integer k such that there are n solutions is $(n+1)(ab)$. Proof is left as an exercise for the reader.

4.2 Factorization

Make tables

5 Prime counting ϕ

5.1 Legendre's prime counting function

If you are familiar with combinatorics, Legendre devised a method for counting primes based on the inclusion-exclusion principle.

In an apparent abuse of notation, let

$$A(x, \prod_{p \in S} p) = x - \lfloor \frac{x}{p_1} \rfloor - \lfloor \frac{x}{p_2} \rfloor ... + \lfloor \frac{x}{p_1 p_2} \rfloor + \lfloor \frac{x}{p_1 p_3} \rfloor ... - \lfloor \frac{x}{p_1 p_2 p_3} \rfloor ... + \lfloor \frac{x}{p_1 p_2 p_3 p_4} \rfloor ...$$

Legendre's method can be broken down $\phi(1000, 2 \cdot 3 \cdot 5) \to 33 \cdot \phi(30, 2 \cdot 3 \cdot 5) + \phi(10, 2 \cdot 3 \cdot 5) = 33 \cdot \phi(30) + \phi(10, 2 \cdot 3 \cdot 5)$

5.2 Meissel's prime counting function

Improving on the inefficacies of Legendre's method, Meissel proposed another prime counting function.

Let S be the set of primes $\leq \sqrt[3]{n}$.

We start with Legendre's method:

$$A(n, \prod_{p \in S} p)$$

where $\prod_{p \in S} m$ are the primes of the set multiplied by each other. To the astute observer, this is $\phi(n)$. Then sieve the primes larger than $\sqrt[3]{n}$.

5.3 Totient function ϕ

$$\phi(p) = p - 1$$
$$\phi(p^2) = p^2 - p$$
$$\phi(p^3) = p^3 - p^2$$

5.4 Prime counting π

Text here

5.5 Mobius function

The mobius function, represented by μ is defined

$$\mu(n) = \begin{cases} 1 & n \text{ an even number of primes} \\ 0 & n \mid k^2, \text{ where } k \text{ is any integer} \\ -1 & n \text{ an odd number of primes} \end{cases}$$

6 Congruences

Congruences are of the form $x = a \pmod{n}$. Linear congruences are of power 1 (x), while quadratics are of the form $x^2 = a \pmod{n}$...

6.1 Systems of multiple variables

Text here

6.2 Chinese Remainder Theorem

To find a solution to a systems of congruences with coprime moduli, we can use the Chinese remainder theorem. We may also break down a congruence with composite modulus into prime moduli by working in reverse.

6.2.1 The orthodox way

For a composite of two primes, say for instance

$$x = a \pmod{35} = \begin{cases} x = 3 & \pmod{5} \\ x = 4 & \pmod{7} \end{cases}$$

We will need to find multiples of 5 and 7 such that $5k + 7\ell = 1$. Fortunately, the integers 15 and -14 appear on light introspection. We can then pair these up with the opposite remainders, such that we have $4(15) - 3(14) = 18 \pmod{35}$. We can repeat these steps even for larger moduli, assuming that it is trivial to find those solutions using the egcd function.

6.2.2 The Sris way

Text here

7 Fermat and Wilson's theorems

Although Fermat had many theorems to his name, here only his little theorem is important to us. A single theorem, it may be written multiple ways:

The first, the additive version, is of the form

$$a^p = a \pmod p$$

Proof. Text here ☐

The second, the multiplicative version, is of the form

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

Where $(a, p) = 1$.

Proof. By example, choose $n = 2$ and $p = 7$. We see that $n^{p-1} \cdot n! = n! \pmod p$.

$$\begin{aligned} 1 \cdot 2 &= 2 \pmod 7 \\ 2 \cdot 2 &= 4 \pmod 7 \\ 3 \cdot 2 &= 6 \pmod 7 \\ 4 \cdot 2 &= 1 \pmod 7 \\ 5 \cdot 2 &= 3 \pmod 7 \\ 6 \cdot 2 &= 5 \pmod 7 \\ 6! \cdot 2^{p-1} &= 6! \pmod 7 \end{aligned}$$

☐

7.1 Wilson's theorem

Another theorem useful to know is Wilson's theorem, which is of the form

$$(p-1)! = -1 \pmod p$$

7.2 Perfect numbers

A number n is perfect if $\sigma(n) = 2n$, where σ is the sum of the positive divisors of n. Some examples are $6, 28, 496, 8128$.

7.3 Extra

- If n is composite, then $2^n - 1$ is composite. Verify this! (Note: It is not as straightforward as one thinks)
- Euclid conjectured that if $1 + 2 + 2^2 + ... + 2^n$ is prime, then $2^n(1 + 2 + 2^2 + ... + 2^n)$ is perfect. Verify this!

8 Primitive roots, discrete logarithms

A primitive root (p–root) is an element that is of the form $|a|_{(p-1)} \pmod p$. In English, this is read "a has order of $p-1$ mod p".

From the textbook: "No method is known for predicting what will be the smallest positive primitive root of a given prime p, nor is there much known about the distribution of the $\phi(p-1)$ primitive roots amount the least residues modulo p.

8.1 Discrete logarithms

Exponent (e):	1	2	3	4	5	6	7	8	9	10
$2^e \pmod{11}$ (a):	2	4	8	5	10	9	7	3	6	1
$(e, 10)$ (n):	1	2	1	2	5	2	1	2	1	10

Table 1: Powers of $2 \pmod{11}$

We abuse notation again and say that the order of a is $10/n$.

9 Quadratic residues

A quadratic residue q is an integer such that $x^2 = q \mod p$. An integer that does not have a square root is called a nonresidue. It is easy to enumerate several quadratic residues per p; they are the perfect squares.