Review of sections 4.1, 4.5, 4.3, 4.2, 6.1, 6.3, 6.4

4.1 Division, modular arithmetic

If we divide 82 by 7 we get

$$\begin{array}{rl} 11 & \leftarrow \text{quotient} \\ 7\,\overline{)\,82} & \\ -7 & \\ \hline 12 & \\ -7 & \\ \hline 5 & \leftarrow \text{remainder} \end{array}$$

and the division algorithm puts these numbers together

$$82 = 7 \cdot 11 + 5 \qquad (a = d \cdot q + \underset{\substack{\uparrow \\ 0 \le r < d}}{r})$$

7 is the divisor
11 is the quotient (82 div 7)
5 is the remainder (82 mod 7).

$7 \mid 82$ is false because remainder is not zero.

$\uparrow$
"7 divides 82"

Also $a \equiv b \pmod{m}$ means $m \mid (a-b)$.

Example ① Is $129 \equiv 111 \pmod{6}$ true or false?

Solution: $129 - 111 = 18$ and $6 \mid 18$ is true because $18 = 6 \cdot 3 + 0$.
So $129 \equiv 111 \pmod{6}$ is true.

4.5 Applications

We saw credit card numbers have a simple check digit scheme using mod 10.

Pseudorandom numbers can be created with the linear congruential method

seed x_0

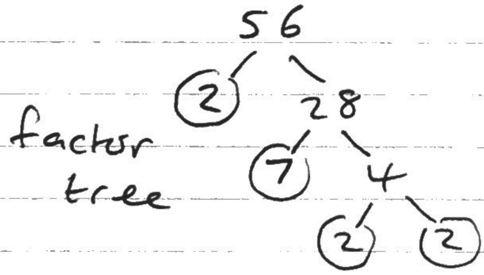
recursion: $x_{n+1} = (\underset{\substack{\uparrow \\ \text{multiplier}}}{a} x_n + \underset{\substack{\uparrow \\ \text{increment}}}{c}) \bmod \underset{\substack{\uparrow \\ \text{modulus}}}{m}$

a, c, m are fixed

You get a random looking sequence $x_0, x_1, x_2, x_3, \ldots$

4.3 Primes, gcds

Any positive integer can be factored into smallest possible integer factors (primes).



so $56 = \underbrace{2 \cdot 2 \cdot 2 \cdot 7}_{\text{prime factorization of } 56}$

To show that a number is prime, check that it has no prime factors up to its square root.

Example ② Show that 101 is prime.

Solution: we have $2, 3, 5, 7 \leq \sqrt{101}$

and $101 \bmod 2 = 1$
$101 \bmod 3 = 2$
$101 \bmod 5 = 1$
$101 \bmod 7 = 3$

So none of 2, 3, 5, 7 divide 101 and it must be prime.

Greatest common divisors

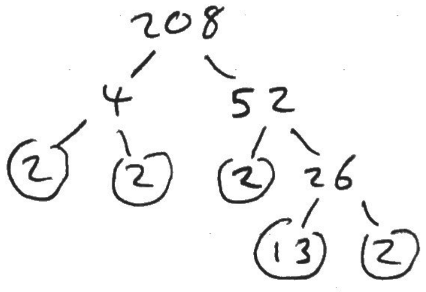
The best way to get the gcd of two numbers uses the **Euclidean Algorithm**. And this means repeating the Division Algorithm until you get a zero remainder.

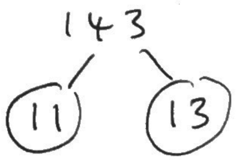
Example ③ Find $\gcd(208, 143)$

$$208 = 143 \cdot 1 + 65$$
$$143 = 65 \cdot 2 + 13$$
$$65 = 13 \cdot 5 + 0 \quad \text{can stop}$$

The gcd is the last nonzero remainder:
$\gcd(208, 143) = 13.$

We can check this is right:





$208 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot \underline{13}$
$143 = 11 \cdot \underline{13}$

4.2 Different bases

A **base b** representation of an integer $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$ means the digits are multiplied by powers of b instead of 10.

So $(562)_7$ means $5 \cdot 7^2 + 6 \cdot 7 + 2 \cdot 1$

$= 289$

$(ABC)_{16}$ means $A \cdot 16^2 + B \cdot 16 + C \cdot 1$

$A=10, B=11, C=12, D=13$ $\quad = 10 \cdot 16^2 + 11 \cdot 16 + 12 \cdot 1$

$E=14, F=15$

$= 2784$

To go the other way keep dividing by the base.

Example ④ Convert 289 to base 7.

Solution:

$$\begin{array}{r} 41 \\ 7\overline{)289} \\ -28 \\ \hline 09 \\ -7 \\ \hline 2 \end{array} \longrightarrow \begin{array}{r} 5 \\ 7\overline{)41} \\ -35 \\ \hline 6 \end{array} \longrightarrow \begin{array}{r} 0 \\ 7\overline{)5} \\ -0 \\ \hline 5 \end{array}$$

The remainders give the digits in reverse order:

$$289 = (562)_7$$

(For any remainders > 9 use the letters A, B, C..).

6.1 Counting

We are counting all the ways something can happen or all the ways some choices can be made. Break it into steps or tasks.

Example ⑤ How many ways can you order a chinese meal if there are 30 meal choices each with white or brown rice and 5 possible sodas?

Solution:

task 1	choose meal	30 ways
task 2	choose rice	2 ways
task 3	choose soda	5 ways

The Product rule says to multiply in this situation, so $30 \cdot 2 \cdot 5 = 300$ ways to order:

List $m_1 r_1 s_1$, $m_1 r_1 s_2$, - - - , $m_{30} r_2 s_5$

Suppose you are only going to order one item from the 30 meals, 2 types of rice and 5 sodas. How many ways to do this?

Now there is only one task and the Sum rule says to add in this situation,

so $30 + 2 + 5 = 37$ ways to order one item.

One more rule: If a task can be done in X ways or Y ways, and Z of these ways are the same, then there are

$$X + Y - Z$$

ways to do the task.

This is called the subtraction rule or the inclusion - exclusion principle.

Example ⑥ In a group of 50 people, suppose 30 have been to Maine and 25 have been to Alaska. If 10 have been to both states, how many have been to Maine or Alaska?

Solution: Your task is choosing people that have been to Maine or Alaska.

$$\underbrace{30}_{\text{Maine}} + \underbrace{25}_{\text{Alaska}} - \underbrace{10}_{\text{same people}} = 45$$

We can also see that 5 in the group haven't been to either state.

6.3 Permutations, combinations

If there are n things, the number of ways to arrange r of them is

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$$

Permutations

product of r numbers going down from n.

Example ⑦ A festival is choosing 4 bands out of 10 available for a concert. How many possible line ups can the concert have?

Solution: Here the order of the bands matters. There are $P(10,4) = 10 \cdot 9 \cdot 8 \cdot 7$

$= 5040$

possible line ups.

If there are n things and you want to choose r of them, not caring about the order, then there are

$$C(n,r) = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r(r-1)\cdots 2 \cdot 1}$$

Combinations

ways to choose.

Example ⑧ Suppose 10 people are at a restaurant together and 4 of them order dessert after the meal. How many ways could this happen?

Solution: Now the order does not matter. So we need combinations

$$C(10,4) = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2 \cdot 1} = \frac{10 \cdot \overset{3}{\cancel{9}} \cdot \cancel{8} \cdot 7}{\cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1} = 210$$

There are 210 ways that 4 of the 10 could order dessert.

6.4 Binomial coefficients

$C(n,r) = \binom{n}{r}$ "n choose r"

notation

example of the binomial theorem

$$(x+y)^4 = \binom{4}{0}x^4y^0 + \binom{4}{1}x^3y^1 + \binom{4}{2}x^2y^2 + \binom{4}{3}x^1y^3 + \binom{4}{4}x^0y^4$$

$$= 1\cdot x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + 1\cdot y^4$$

for example, replacing x by $2x$ and y by -1 we get

$$(2x-1)^4 = 1(2x)^4 + 4(2x)^3(-1) + 6(2x)^2(-1)^2$$

$$+ 4(2x)(-1)^3 + 1\cdot(-1)^4$$

$$= 16x^4 - 32x^3 + 24x^2 - 8x + 1.$$

we also looked at Pascal's identity and Pascal's triangle.