Chapter 4 Number theory + Cryptography

4.1 Divisibility and modular arithmetic

Here are some examples of division:

$$27 \div 3 = 9 \qquad 11 \div 11 = 1 \qquad 61 \div 7 = 8.714\ldots$$

Why is the last one a decimal? The problem is that 7 does not fit evenly into 61

$$\begin{array}{r} 8 \\ 7\,\overline{)\,61} \\ -56 \\ \hline 5 \end{array}$$

8 ← quotient

5 ← remainder

7 fits into 61 8 times with remainder 5

For the first two there was no remainder and we say 3 divides 27 (means divides evenly) and 11 divides 11. 7 does not divide 61.

Notation: $3 \mid 27 \qquad 11 \mid 11 \qquad 7 \nmid 61$

Example ① Are these true? $9 \mid 206$, $7 \mid 217$

Solution:

$$\begin{array}{r} 22 \\ 9\,\overline{)\,206} \\ -18 \\ \hline 26 \\ -18 \\ \hline 8 \end{array} \qquad\qquad \begin{array}{r} 31 \\ 7\,\overline{)\,217} \\ -21 \\ \hline 07 \\ -7 \\ \hline 0 \end{array}$$

remainder $\neq 0$ → 8

so $9 \mid 206$ is false

$(9 \nmid 206)$.

$7 \mid 217$ is true.

Let a, b be integers (with $a \neq 0$) then

$a \mid b$ is the same as saying

a is a factor of b
b is a multiple of a
$b = ac$ for some integer c

Example ② Is $17 \mid 0$ true?

Solution: Yes it's true $17 \cdot 0 = 0$. (Every nonzero integer divides 0.)

The division algorithm

If you divide an integer by 9 what are the possible remainders?

We saw remainder 8 in ex ①. The remainder could not be bigger than 8 or else 9 fits in more times. So if you divide any integer by 9 the remainder must be

$$0, 1, 2, 3, 4, 5, 6, 7 \text{ or } 8.$$

In our example $206 \div 9 = 22 \text{ R } 8$

and we can write this as

$$206 = \underset{\text{divisor}}{9} \cdot \underset{\text{quotient}}{22} + \underset{\text{remainder.}}{8}$$

The next result is really a fundamental theorem and not an algorithm.

The division algorithm: Let a be an integer and d a positive integer. Then there are unique integers q and r so that

$$a = dq + r \quad \text{and} \quad 0 \le r < d.$$

Example ③ Find the quotient q and remainder r when $a = 218$ is divided by $d = 3$.

Solution:

$$\begin{array}{r} 72 \\ 3\overline{)218} \\ -21 \\ \hline 08 \\ -6 \\ \hline 2 \end{array}$$

so $q = 72$, $r = 2$

and

$$218 = 3 \cdot 72 + 2.$$

We can follow the book's notation for quotient and remainder

$$\boxed{q = a \text{ div } d} \qquad \boxed{r = a \text{ mod } d}$$

Here "div" is short for division and "mod" short for modulo (measuring in Latin).

So $\quad 218 \text{ div } 3 = 72, \quad 218 \text{ mod } 3 = 2.$

- See examples 3, 4 p 239.

Modular arithmetic

Suppose it is 9 on a 24 hour clock (so 9am). What time will it be in 100 hours?
Since the time goes back to 0 every 24 hours we only need the remainder after dividing by 24:

$$\begin{array}{r} 4 \\ 24\overline{)\,109} \\ -\,96 \\ \hline 13 \end{array}$$

so the answer is 13 hours (1 pm).

A second way to do this problem is to see that $100 \bmod 24 = 4$

$$\begin{array}{r} 4 \\ 24\overline{)\,100} \\ -\,96 \\ \hline 4 \end{array}$$

so adding 100 hours to 9 looks the same as adding 4 hours on a 24-hour clock. $9+4=13$ again.

In this clock example we are dividing by 24 and this is called the modulus.
For times we only need the remainders after dividing by this modulus. If two integers a and b represent the same time we can write

$$a \equiv b \pmod{m} \qquad m=24 \text{ here}$$

"a is congruent to b modulo m"

Definition: Let a, b be integers and m any positive integer. Then $a \equiv b \pmod{m}$ means m divides $a-b$.

Example ④ Show that $253 \equiv 169 \pmod{7}$.

Solution: Here $a = 253$, $b = 169$, $m = 7$.
$a - b = 253 - 169 = 84$

$$\begin{array}{r} 12 \\ 7 \overline{)84} \\ -7 \\ \hline 14 \\ -14 \\ \hline 0 \end{array}$$

7 divides $a - b = 84$

so $253 \equiv 169 \pmod{7}$ is true.

- See example 5 p 241.

The notation $\equiv$ is similer to $=$ and indicates that there is something the "same" about 253 and 169. what do they have in common?

Answer - they have the same remainder when you divide by the modulus 7:

Check that $253 \bmod 7 = 1$
$169 \bmod 7 = 1$

In general

$$\boxed{a \equiv b \pmod{m} \longleftrightarrow a \bmod m = b \bmod m}$$

Example 5 Find 101 mod 3 and 208 mod 3. Use those results to decide if 101 is congruent to 208 modulo 3.

Solution: 101 mod 3 means the remainder when 101 is divided by 3

$$\begin{array}{r} 33 \\ 3\overline{)101} \\ -9 \\ \hline 11 \\ -9 \\ \hline 2 \end{array} \longrightarrow \quad 101 \bmod 3 = 2$$

$$\begin{array}{r} 69 \\ 3\overline{)208} \\ 18 \\ \hline 28 \\ -27 \\ \hline 1 \end{array} \longrightarrow \quad 208 \bmod 3 = 1$$

They have different remainders so 101 is not congruent to 208 modulo 3

$$101 \not\equiv 208 \pmod 3.$$

• See p 242 for adding and multiplying in modular arithmetic.