The division algorithm

Let $a \geq 1$ be an integer. For any integer $n$ there exist integers $q$ and $r$ such that $n = aq + r$ and $0 \leq r \leq a-1$. Moreover, $q$ and $r$ are uniquely determined by $n$ and $a$.

Remarks: (1) Division algorithm is a theorem, not an algorithm. An algorithm for finding $q$ and $r$ in the case where $n$ is positive, is called long division.

(2) $n$ is divisible by $a$ if and only if $r=0$. One direction is obvious: if $r=0$, then $n = aq$ is divisible by $a$. Conversely, if $n$ is divisible by $a$, say $n = ab$, then $n = aq + r$. By the uniqueness part of theorem, $b = q$, $r = 0$. 
(3) If \( n \geq 0 \), then the division algorithm is the same thing as writing \( \frac{n}{a} \) as a mixed fraction: \( \frac{n}{a} = q + \frac{r}{a} \).

**Proof using well-ordering principle:**

First assume that \( n \geq 0 \). We want to show that there exist integers \( q \) and \( r \) such that \( n = aq + r \), and \( 0 \leq r \leq a-1 \). Assume the contrary: not every \( n \geq 1 \) can be written this way. By well-ordering principle there exists smallest such \( n \).

Claim: \( n \geq a \).

Indeed, any \( 0 \leq m \leq a-1 \) can be written as \( n = a \cdot 0 + n \), with \( q = 0 \) and \( r = n \). This proves claim.

Now \( 0 \leq n - a < n \). Thus \( n - a = aq + r \) where \( 0 \leq r \leq a-1 \). Now \( n = a(q + 1) + r \)
This shows that \( n \) can be written in the form \( aq + r \) with \( 0 \leq r \leq a-1 \), contrary to our assumption. This proves the existence part of division algorithm for \( n \geq 0 \).

If \( n < 0 \), choose an integer \( x \) such that \( x \geq \frac{n}{a} \), say \( x = n \).

Replace \( n \) by \( n + xa \). By our choice of \( x \), \( n + xa \) is a positive integer.

Thus \( n + xa = aq + r \), for some integers \( q \), \( r \), with \( 0 \leq r \leq a-1 \).

Now \( n = a(q-x) + r \) can be expressed in the form we want. This completes the proof of existence part of division algorithm.
For uniqueness, assume
\[ n = aq_1 + r_1 \quad 0 \leq r_1 \leq a - 1 \]
\[ n = aq_2 + r_2 \quad 0 \leq r_2 \leq a - 1 \]
May assume that \( r_1 \geq r_2 \); otherwise interchange \((q_1, r_1)\) and \((q_2, r_2)\).
Subtract: \[ 0 = a(q_1 - q_2) + (r_1 - r_2) \]
\[ a(q_2 - q_1) = r_1 - r_2, \]
Multiple of a integer between 0 and a - 1
A contradiction, unless \( r_1 - r_2 = 0 \).
Thus \( r_1 = r_2 \) and \( a(q_2 - q_1) = 0 \)
\[ q_1 = q_2. \] This proves uniqueness
Q.E.D.
Examples: (1) \( n = 30, \ a = 7 \).
What are \( q \) and \( r \) in this case?
\( q = 4, \ r = 2 \) \hspace{1cm} 30 = 7 \cdot 4 + 2

\[
\frac{30}{7} = 4 + \frac{2}{7}
\]

(2) \( n = 17, \ a = 3 \). What are \( q \) and \( r \)?
\( q = 5, \ r = 2 \) \hspace{1cm} 17 = 3 \cdot 5 + 2

(3) \( n = -17, \ a = 3 \)
\( q = -6, \ r = 1 \) \hspace{1cm} -17 = 3 \cdot (-6) + 1
Primes: 2, 3, 5, 7, 11, 13, 17, ...

No formula for the nth prime.

**Theorem (Euclid):** There are infinitely many primes.

**Proof:** Assume the contrary: there are only finitely many primes, $p_1, \ldots, p_k$. Let

$$n = p_1 p_2 \cdots p_k + 1$$

$n > p_1, \ldots, p_k \Rightarrow n$ is not a prime.

Last time we showed that $n$ is a product of primes. Thus $n$ is divisible by some prime, say by $p_i$.

On the other hand

$$n = p_i (p_1 \cdots p_{i-1} p_{i+1} \cdots p_k) + 1$$

remainder
This shows that \( n \) is not divisible by \( p_i \), a contradiction. Q.E.D.

Example: \( 2 \cdot 3 \cdot 5 + 1 = 31 \) new prime
\( 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \) another prime

A better practical way to generate primes: sieve of Eratosthenes.

Key idea: If \( n = a \cdot b \) is composite, then at least one of \( a, b \) is \( \leq \sqrt{n} \).

To find primes \( \leq 25 \), only need to check divisibility by 2, 3, and 5.
Cross out numbers divisible by 2 (starting from 4)
by 3 (starting from 6)
by 5 (starting from 10)

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23

Can repeat this to find all primes up to 625.
Prime number theorem:

The number of primes in \([2, x]\) is approx. \(\frac{x}{\ln(x)}\).

In other words, the probability that a randomly selected integer in \([2, x]\) is a prime is \(\frac{1}{\ln x}\) (for large \(x\)).