Integers and Integer Algorithms

1. If a and b are integers with $a \neq 0$, we say a *divides* b if there is an integer k such that $b = ak$. a is called a *factor* of b and b is a *multiple* of a.

   Notation: $a \mid b$ when a divides b. $a \nmid b$ when a does not divide b.

2. Examples: (a) $3 \mid 12$. (b) $3 \nmid 7$.

3. Theorem: Let a, b, c be integers, then
   - if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
   - if $a \mid b$, then $a \mid bc$ for all integers c
   - if $a \mid b$ and $b \mid c$, then $a \mid c$

   Proof: .... (do-it-yourself)

4. Theorem ("The Division Algorithm"): given integers a, $d > 0$, there is a unique q and r, such that
$$a = d \cdot q + r, \quad 0 \leq r < d.$$
   d is referred to as "divisor", q is "quotient" and r is "remainder".

5. Modular arithmetic: $a \bmod d = r =$ the remainder after dividing a by d.

6. Examples:

   (a) $7 \bmod 3 = 1$, since $7 = 3 \cdot 2 + 1$. (b) $3 \bmod 7 = 3$, since $3 = 7 \cdot 0 + 3$

   (c) $-133 \bmod 9 = 2$, since $-133 = 9 \cdot (-15) + 2$. (Note: the remainder $r = a \bmod d$ cannot be negative. Consequently, in this example, the remainder is not -2, even though $-11 = 3 \cdot (-3) - 2$, because $r = -2$ does not satisfy $0 \leq r < 3$.)

7. If a and b are integers, and m is a positive integer, then a is *congruent to* b *modulo* m if $m|(a - b)$.

   notation: $a \equiv b \pmod{m}$

8. Examples: (a) $17 \equiv 5 (\text{mod } 6)$, (b) $24 \not\equiv 14 (\text{mod } 6)$.

9. Mudular arithmetic: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then (a) $a + c \equiv b + d \pmod{m}$. (b) $ac \equiv bd \pmod{m}$

10. A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.

    e.g.: 2, 3, 5, 7, 11, 13, ... are primes.

11. The Fundamental Theorem of Arithmetic ("prime factorization"): Every positive integer greater than 1 can be written uniquely as the product of primes, where the prime factors are written in order of increasing size.

    For examples: (a) $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$. (b) $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$. (c) $1024 = 2^{10}$

12. Let a and b be integers, not both zero. The *largest* integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* (gcd) of a and b. notation: $\gcd(a, b) = d$.

13. Examples:

    (a) $\gcd(24, 36) = 12$, since the positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, 12.

    (b) $\gcd(17, 22) = 1$, since 17 is a prime. (c) $\gcd(1, 123) = 1$ (d) $\gcd(0, 321) = 321$

14. If $\gcd(a, b) = 1$, then a and b are *relatively prime*.

15. First algorithm for computing $\gcd(a, b)$:

    1) compute the prime factorization $a = 2^{n_1}3^{n_2}5^{n_3}\cdots$

    2) compute the prime factorization $b = 2^{m_1}3^{m_2}5^{m_3}\cdots$

    3) $\gcd(a, b) = 2^{\min\{n_1,m_1\}}3^{\min\{n_2,m_2\}}5^{\min\{n_3,m_3\}}\cdots$

16. Example: $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$

    $\gcd(120, 500) = 2^{\min\{3,2\}}3^{\min\{1,0\}}5^{\min\{1,3\}} = 2^2 3^0 5^1 = 20$

17. **Theorem**: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

    Proof: If we can show the following set identity:

    (*) "the set of common divisors of a and b" = "the set of common divisors of b and r"

    Then we will have shown that $\gcd(a, b) = \gcd(b, r)$, since both pairs must have the same greatest common divisor.

    To show (*),

    - let $d \mid a$ and $d \mid b$, then $d \mid bq$. It follows that then $d \mid a - bq$. Therefore $d \mid b$ and $d \mid r$.
    - On the other hand, let $d \mid b$ and $d \mid r$, then $d \mid bq$. It follows that then $d \mid bq + r$. Therefore, $d \mid a$ and $d \mid b$. $\diamond$

18. Let $r_0 = a$ and $r_1 = b$. When we successively apply "The Division Algorithm", we obtain

$$
\begin{aligned}
a = r_0 &= r_1 \cdot q_1 + r_2, && 0 \le r_2 < r_1 = b, \\
r_1 &= r_2 \cdot q_2 + r_3, && 0 \le r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, && 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n \cdot q_n + 0.
\end{aligned}
$$

Eventually, a remainder of zero must occur, since the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \ge 0$ cannot contain more than a terms. i.e. $n \le a$, As a result, by the theorem, it follows that

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

19. The Euclidean algorithm

```
procedure gcd(a,b: positive integers)
x := a
y := b
while y /= 0
   r := x mod y
   x := y
   y := r
end while
return x      % x is the gcd(a,b)
```

20. Complexity: the number of divisions required by the Euclidean algorithm is $O(\log b)$, where $a \ge b > 0$