Discrete Mathematics

Supervision 3

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

3. More on numbers

3.1. Basic exercises

1. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
2. Find the gcd of 21212121 and 12121212.
3. Prove that for all positive integers m and n, and integers k and l,

$$\gcd(m,n) \mid (k \cdot m + l \cdot n)$$

4. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \le y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.
5. Prove that for all positive integers m and n, there exists integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m, n) = 1$.
6. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod p$ then either $n \equiv 1 \pmod p$ or $n \equiv -1 \pmod p$.

3.2. Core exercises

1. Prove that for all positive integers m and n, $\gcd(m, n) = m$ iff $m \mid n$.
2. Let m and n be positive integers with $\gcd(m, n) = 1$. Prove that for every natural number k,

$$m \mid k \wedge n \mid k \iff m \cdot n \mid k$$

3. Prove that for all positive integers a, b, c, if $\gcd(a, c) = 1$ then $\gcd(a \cdot b, c) = \gcd(b, c)$.
4. Prove that for all positive integers m and n, and integers i and j:

$$n \cdot i \equiv n \cdot j \pmod m \iff i \equiv j \left(\mathrm{mod}\ \frac{m}{\gcd(m,n)}\right)$$

5. Prove that for all positive integers m, n, p, q such that $\gcd(m, n) = \gcd(p, q) = 1$, if $q \cdot m = p \cdot n$ then $m = p$ and $n = q$.
6. Prove that for all positive integers a and b, $\gcd(13 \cdot a + 8 \cdot b, 5 \cdot a + 3 \cdot b) = \gcd(a, b)$.
7. Let n be an integer.
   a) Prove that if n is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.
   b) Show that if n is odd, then $n^2 \equiv 1 \pmod 8$.
   c) Conclude that if p is a prime number greater than 3, then $p^2 - 1$ is divisible by 24.

8. Prove that $n^{13} \equiv n \pmod{10}$ for all integers n.
9. Prove that for all positive integers l, m and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.
10. Solve the following congruences:

    a) $77 \cdot x \equiv 11 \pmod{40}$

    b) $12 \cdot y \equiv 30 \pmod{54}$

    c) $\begin{cases} 13 \equiv z \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

11. What is the multiplicative inverse of: (a) 2 in $\mathbb{Z}_7$, (b) 7 in $\mathbb{Z}_{40}$, and (c) 13 in $\mathbb{Z}_{23}$?
12. Prove that $\left[22^{12001}\right]_{175}$ has a multiplicative inverse in $\mathbb{Z}_{175}$.

3.3. Optional exercises

1. Let a and b be natural numbers such that $a^2 \mid b \cdot (b + a)$. Prove that $a \mid b$.

   Hint: For positive a and b, consider $a_0 = \frac{a}{\gcd(a,b)}$ and $b_0 = \frac{b}{\gcd(a,b)}$ so that $\gcd(a_0, b_0) = 1$, and show that $a^2 \mid b(b + a)$ implies $a_0 = 1$.

2. Prove the converse of §1.3.1(f): For all natural numbers n and s, if there exists a natural number q such that $(2n + 1)^2 \cdot s + t_n = t_q$, then s is a triangular number. (49th Putnam, 1988)

   Hint: Recall that if (†) $q = 2nk + n + k$ then $(2n + 1)^2\, t_k + t_n = t_q$. Solving for k in (†), we get that $k = \frac{q-n}{2n+1}$; so it would be enough to show that the fraction $\frac{q-n}{2n+1}$ is a natural number.

3. Informally justify the correctness of the following alternative algorithm for computing the gcd of two positive integers:

```
let rec gcd0(m, n) = if m = n then m
                     else let p = min m n
                          and q = max m n
                           in gcd0(p, q - p)
```