Greatest common divisor

Exercises

Application of discrete models

Mathematical questions

1. Define the greatest common divisor of two numbers. Demonstrate the definition on 6 and 4.

2. Define the least common multiple of two numbers. Demonstrate the definition on 6 and 4.

3. When are two numbers coprime? Give *three* examples for such an x that 12 and x are coprime.

4. Are 4, 5 and 6 coprime? Are they *pairwise* coprime?

5. Calculate the greatest common divisor and least common multiple of 200 and 120 using their prime factorization.

6. Calculate the following using the Euclidean algorithm:
a) $\gcd(39, 15)$; b) $\gcd(32, 20)$; c) $\gcd(12, 7)$; d) $\gcd(200, 120)$; e) $\gcd(39, 30)$;
f) $\gcd(125, 90)$; g) $\gcd(157, 15)$; h) $\gcd(102, 72)$; i) $\gcd(55, 34)$; j) $\gcd(700, 300)$.

7. Perform the *extended* Euclidean algorithm for the above pairs of numbers. Write down the resulting equality in each case.

8. Give *one* solution for each of the following linear Diophantine equations (where possible):
a) $39x + 15y = 6$; b) $32x + 20y = 10$; c) $12x + 7y = -4$; d) $200x + 120y = 4000$.

9. Express *all* solutions of the above linear Diophantine equations.

10. On an island, there are 7-headed and 12-headed dragons. The total number of dragon heads is 100. How many dragons are on the island? Solve it using linear Diophantine equations.

Programming exercises

11. Write a function that calculates the greatest common divisor of $a, b \in \mathbb{N}^+$

a) from their prime factorization (`factor()`);

b) using the *naive* version of the Euclidean algorithm (i.e. by subtractions);

c) using the Euclidean algorithm (i.e. by remainder calculations).

Test the solutions for all pairs of numbers between 1 and 50. Which methods work for 0?

12. Compare the running time of the above solutions as follows.

a) Let a and b be the products of two big prime numbers, more precisely $a := pq$ and $b := pr$, where p, q and r are three random prime numbers. The primes are between 2 and 10^n, where n is an increasingly bigger exponent: $n = 2, 3, 4, \ldots, 40$. (So a and b are roughly of the same order of magnitude, and they are constructed so that $\gcd(a, b) = p$.) Which solution is usable for how big n?

b) Modify the previous tests by making b much smaller than a, more precisely let r be always between 2 and 100, while p and q remain between 2 and 10^n. What has changed?

13. Write a function that calculates $\operatorname{lcm}(a, b)$ from $\gcd(a, b)$. Test the function for all pairs of numbers between 0 and 50.

14. Write a function that calculates $\gcd(a_1, a_2, \ldots, a_n)$ using the bivariate $\gcd(a, b)$. The function receives the numbers in a list.

15. Implement the extended Euclidean algorithm: write a function that, for given $a, b \in \mathbb{N}^+$, calculates $\gcd(a, b)$ and the Bézout coefficients for a and b.

16. Consider the linear Diophantine equation $ax + by = c$, where $a, b, c \in \mathbb{N}^+$ are input parameters, are solve the following exercises for it. For testing, the equations from questions 8 and 10 above can be used, and test it also for the following equation:

$$12345678x + 89009765y = 1122334455667788.$$

a) Write a function that calculates one solution of the equation (an (x, y) pair), or returns `None` if no solution exists.

b) Write a function that returns n consecutive solutions (where $n \in \mathbb{N}^+$ is also an input parameter) in a list: $[(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)]$.

c) Write a function that returns all nonnegative solutions in a list.