

Number Theory: Examples Sheet 1 of 4

1. Calculate $d = (a, b)$ and find integers r and s such that $ra + sb = d$ when

(i) $a = 841$, $b = 160$;

(ii) $a = 2613$, $b = 2171$.

Find distinct non-zero integers x, y, z such that $15x + 36y + 77z = 1$.

2. Let a and b be integers with $a > b > 1$. Let $\lambda(a, b)$ denote the number of individual applications of the division algorithm required by Euclid's algorithm to compute the greatest common divisor of a and b .

(i) What is the smallest possible value of $\lambda(a, b)$ for four-digit numbers a and b ?

(ii) Find a pair of four-digit numbers a and b for which $\lambda(a, b) \geq 15$.

(iii) Find constants c and d such that $\lambda(a, b) \leq c \log b + d$.

3. Where possible, give examples of positive integers a, b and c such that the equation $ax + by = c$ has

(i) no integer solution (x, y) ;

(ii) exactly one integer solution (x, y) ;

(iii) infinitely many integer solutions (x, y) .

Briefly justify your answers.

4. Let x be an integer greater than 1. Use the Fundamental Theorem of Arithmetic to show that

$$x \leq \left(1 + \frac{\log x}{\log 2}\right)^{\pi(x)}.$$

Deduce that when $x \geq 8$, we have $\pi(x) \geq \log x / (2 \log \log x)$.

5. Let a and n be integers greater than 1. Prove that if $a^n - 1$ is prime, then $a = 2$ and n is prime.

6. Let q be an odd prime. Prove that every prime factor of $2^q - 1$ must be congruent to 1 mod q , and also congruent to ± 1 mod 8. Use this to factor $2^{11} - 1 = 2047$.

7. We say that a positive integer n is *perfect* if the sum of all the positive divisors of n is equal to $2n$. Prove that a positive even integer n is perfect if and only if it can be written in the form $n = 2^{q-1}(2^q - 1)$, where $2^q - 1$ is prime.

(It is conjectured that there are no odd perfect numbers, but this is as yet unknown.)

8. By considering numbers of the form $n = (2^2 \cdot 3 \cdot 5 \cdots p) - 1$, prove that there are infinitely many primes congruent to 3 mod 4.
9. Find the smallest non-negative integer x satisfying the congruences $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{11}$, $x \equiv 5 \pmod{16}$.
10. Find all integers x satisfying both $19x \equiv 103 \pmod{900}$ and $10x \equiv 511 \pmod{841}$.
11. Prove that the classes of both 2 and 3 generate $(\mathbb{Z}/5^n\mathbb{Z})^\times$ for all positive integers n . For each of the primes $p = 11, 13, 17$ and 19 , find a generator of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for all $n \geq 1$.
12. Let A be the group $(\mathbb{Z}/65520\mathbb{Z})^\times$. Determine the least positive integer n such that $g^n = 1$ for all g in A .
13. Let a and n be integers greater than 1, and put $N = a^n - 1$. Show that the order of $a + N\mathbb{Z}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is exactly n , and deduce that n divides $\phi(N)$. If n is a prime, deduce that there are infinitely many primes q such that $q \equiv 1 \pmod{n}$.