

1. Find all integer solutions of the equation  $987x + 567y = 63$ .

$$\begin{array}{r} 987 \quad 1 \quad 0 \\ 567 \quad 0 \quad 1 \\ 420 \quad 1 \quad -1 \\ 147 \quad -1 \quad 2 \\ 126 \quad 3 \quad -5 \\ 21 \quad -4 \quad 7 \\ 0 \quad 27 \quad -47 \end{array}$$

We see that  $(u, v) = (-4, 7)$  is a solution of  $987u + 567v = 21 (= \gcd(987, 567))$ . Multiplying by 3, we find that  $(x_0, y_0) = (-12, 21)$  is a solution of our equation, and all solutions are given by

$$(x, y) = (-12, 21) + (27, -47)t, \quad t \in \mathbb{Z}.$$

2. Use the fact that  $1001 = 7 * 11 * 13$  to state a criterion for divisibility by 7, or 11, or 13 (similar to a well-known criterion for divisibility by 3 or 9).

Let  $n \in \mathbb{N}$ , and write  $n$  in base 1000 (i.e. break the decimal representation of  $n$  into parcels of 3 digits, starting from the right):

$$n = a_0 1000^0 + a_1 1000^1 + a_2 1000^2 + \dots$$

Since  $1000 \equiv -1 \pmod{k}$  (where  $k = 7, 11, 13$ ), we see that  $n \equiv a_0 - a_1 + a_2 - a_3 \pm \dots$ , and in particular  $n$  is divisible by  $k$  if and only if this alternating sum is divisible by  $k$ .

E.g.  $n = 22123453$  is not divisible by 7 or 13, but divisible by 11 (look at  $123 - 453 + 22 = 352$ ).

3. Find all solutions of the congruence  $x^3 + x + 2 \equiv 0 \pmod{140}$ .

Factorize:  $140 = 4 * 5 * 7$ . Now find all  $x$  which satisfy all three congruences:  $x^3 + x + 2 \equiv 0 \pmod{4}$ ,  $x^3 + x + 2 \equiv 0 \pmod{5}$ ,  $x^3 + x + 2 \equiv 0 \pmod{7}$ .

We find  $x \equiv 1, 2, 3 \pmod{4}$ ,  $x \equiv 4 \pmod{5}$ ,  $x \equiv 4, 6 \pmod{7}$ . Using the Chinese Remainder Theorem we find  $x \equiv 34, 39, 69, 74, 109, 139 \pmod{140}$ .

4. Let  $p > 4$  be a prime,  $n \in \mathbb{N}$ , and assume that  $\frac{2}{3}n < p \leq n$ . Prove that  $p$  does not divide the binomial coefficient  $\binom{2n}{n}$ .

For prime numbers in the interval  $(\frac{2}{3}n, p]$ , we have  $n < 2p \leq 2n$ , showing that such prime factor occurs exactly once in the numerator and in the denominator. Consequently  $\binom{2n}{n}$  is not divisible by  $p$ .

5. Find the number of positive divisors of  $20!$  (that's 20 factorial).

Calculate the sums  $\sum_{i \in \mathbb{N}} \lfloor \frac{20}{p^i} \rfloor$  for all primes (well, need only look at the primes less than 20, and of those only the ones less than 10 need a calculation):

the highest power of 2 dividing 20 is  $10 + 5 + \lfloor 2.5 \rfloor + \lfloor 1.25 \rfloor = 18$ ;

the highest power of 3 dividing 20 is  $\lfloor 6.7 \rfloor + \lfloor 2.3 \rfloor = 8$ ;

the highest power of 5 dividing 20 is 4;  
the highest power of 7 dividing 20 is 2;  
the highest power of 11, 13, 17, 19 dividing 20 is 1.

Therefore 20 is a product of 8 distinct primes raised to powers 18, 8, 4, 2, 1, 1, 1, 1 respectively.  
The number of positive divisors of 20 is thus  $19 \cdot 9 \cdot 5 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 41040$ .

$$(20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19.)$$

6. Let  $n$  be a perfect number, i.e.  $n$  is a positive integer such that the sum of all positive divisors of  $n$  equals  $2n$ . Prove that

$$\sum_{d|n} \frac{1}{d} = 2.$$

Note that  $\sum_{d|n} d = \sum_{d|n} \frac{n}{d} = n \sum_{d|n} \frac{1}{d}$ . It follows that  $\sum_{d|n} d = 2n/n = 2$ .

7. From Euclid's proof that there are infinitely many primes, deduce that the  $n$ -th prime is less than  $2^{2^n}$  (induction might help).

The statement is obviously true for the first prime ( $2 \leq 2^2$ ). If  $p_k$  denotes the  $k$ -th prime, and we assume the result for  $n = k$ , then Euclid's idea says that the product  $u = p_1 p_2 \cdots p_k + 1$  contains a further prime factor, and therefore  $p_{k+1} \leq u < 2 \cdot 2^2 \cdots 2^k + 1 = 2^{2+2^2+\cdots+2^k} + 1 = 2^{2^{k+1}-1} + 1 < 2^{2^{k+1}}$ . So the statement is also true for  $n = k + 1$ .

8. For  $n \in \mathbb{N}$ , define  $d(n)$  to be the number of positive divisors of  $n$ . Prove that  $d$  is a multiplicative function, i.e. if  $\gcd(m, n) = 1$  then  $d(mn) = d(m)d(n)$ .

If  $m$  is a product of  $r$  distinct primes  $p_i$ , each raised to power  $\alpha_i$ , then the number of positive divisors of  $m$  is  $d(m) = \prod (\alpha_i + 1)$ . If  $n$  is a product of  $s$  distinct primes  $q_i$ , each raised to power  $\beta_i$ , then the number of positive divisors of  $n$  is  $d(n) = \prod (\beta_i + 1)$ . If  $m$  and  $n$  are relatively prime, then the prime factors of  $m$  and  $n$  are distinct, so  $mn$  is a product of  $r + s$  distinct primes  $p_i$  or  $q_i$ , each raised to power  $\alpha_i$  or  $\beta_i$ , and the number of positive divisors of  $mn$  is  $d(mn) = \prod (\alpha_i + 1) \prod (\beta_i + 1) = d(m)d(n)$ .

9. Show that there are infinitely primes of the form  $4n + 3$  ( $n \in \mathbb{N}$ ). (Dirichlet's theorem guarantees that — but find a more elementary approach.)

(A variation on Euclid's proof that there are infinitely many primes.) Assume that  $p$  is the largest prime of the form  $4n + 3$  and form the product of all primes up to  $p$ , then put  $N = 4 \cdot 3 \cdot 5 \cdots p - 1$ . Then  $N \equiv 3 \pmod{4}$ , and at least one of the prime factors of  $N$ , say  $q$ , must be  $\equiv 3 \pmod{4}$  (since the product of numbers congruent to 1 mod 4 is again congruent to 1 mod 4).  $q$  cannot be any of the primes  $\leq p$ , so there is a prime of the required form which is  $> p$ , a contradiction.

10. True or false:  $x^2 - x + 41$  is prime for all  $x \in \mathbb{N}$ .

(Just a joke exercise. This polynomial is associated with the name of Euler, producing prime numbers for all values of  $x$  that are  $< 41$ .)

False: e.g. try  $x = 41$ , then  $41|x^2 - x + 41$ .