

1. For each pair of integers (a, b) , use the Euclidean algorithm to calculate their greatest common divisor $d = \gcd(a, b)$ and also to find integers x and y such that $d = xa + yb$.

(a) $a = 44, b = 12$.

- Applying the Euclidean algorithm to $a = 44$ and $b = 12$ yields

$$44 = 3 \cdot 12 + 8$$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4$$

and thus the gcd is the last nonzero remainder of $\boxed{4}$.

- For the linear combination, we solve for the remainders:

$$8 = 1 \cdot 44 - 3 \cdot 12$$

$$4 = 12 - 1 \cdot 8 = -1 \cdot 44 + 4 \cdot 12$$

and so we see $\boxed{4 = -1 \cdot 44 + 4 \cdot 12}$ so we can take $x = -1$ and $y = 4$.

(b) $a = 481, b = 24$.

- Applying the Euclidean algorithm to $a = 481$ and $b = 24$ yields

$$481 = 20 \cdot 24 + 1$$

$$24 = 24 \cdot 1$$

and thus the gcd is the last nonzero remainder of $\boxed{1}$.

- For the linear combination, we trivially solve for the remainder $\boxed{1 = 1 \cdot 481 - 20 \cdot 24}$ so we can take $x = 1$ and $y = -20$.

(c) $a = 18063, b = 2025$.

- Applying the Euclidean algorithm to $a = 18063$ and $b = 2025$ yields

$$18063 = 8 \cdot 2025 + 1863$$

$$2025 = 1 \cdot 1863 + 162$$

$$1863 = 11 \cdot 162 + 81$$

$$162 = 2 \cdot 81$$

and so the gcd is the last nonzero remainder of $\boxed{81}$.

- For the linear combination, we solve for the remainders:

$$1863 = 1 \cdot 18063 - 8 \cdot 2025$$

$$162 = 2025 - 1 \cdot 1863 = -1 \cdot 18063 + 9 \cdot 2025$$

$$81 = 1863 - 11 \cdot 162 = 12 \cdot 18063 - 107 \cdot 2025$$

and so we see $\boxed{81 = 12 \cdot 18063 - 107 \cdot 2025}$ so we can take $x = 12$ and $y = -107$.

(d) $a = 12445, b = 5567$.

- Applying the Euclidean algorithm to $a = 12445$ and $b = 5567$ yields

$$12445 = 2 \cdot 5567 + 1311$$

$$5567 = 4 \cdot 1311 + 323$$

$$1311 = 4 \cdot 323 + 19$$

$$323 = 17 \cdot 19$$

and so the gcd is the last nonzero remainder of $\boxed{19}$.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 1311 &= & &= 1 \cdot 12445 - 2 \cdot 5567 \\ 323 &= 5567 - 4 \cdot 1311 &= &= -4 \cdot 12445 + 9 \cdot 5567 \\ 19 &= 1311 - 4 \cdot 323 &= &= 17 \cdot 12445 - 38 \cdot 5567 \end{aligned}$$

and so we see $\boxed{19 = 17 \cdot 12445 - 38 \cdot 5567}$ so we can take $x = 17$ and $y = -38$.

(e) $a = 18200$, $b = 3505$.

- Applying the Euclidean algorithm to $a = 18200$ and $b = 3505$ yields

$$\begin{aligned} 18200 &= 5 \cdot 3505 + 675 \\ 3505 &= 5 \cdot 675 + 130 \\ 675 &= 5 \cdot 130 + 25 \\ 130 &= 5 \cdot 25 + 5 \\ 25 &= 5 \cdot 5 \end{aligned}$$

and so the gcd is the last nonzero remainder of $\boxed{5}$.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 675 &= & &= 1 \cdot 18200 - 5 \cdot 3505 \\ 130 &= 3505 - 5 \cdot 675 &= &= -5 \cdot 18200 + 26 \cdot 3505 \\ 25 &= 675 - 5 \cdot 130 &= &= 26 \cdot 18200 - 135 \cdot 3505 \\ 5 &= 130 - 5 \cdot 25 &= &= -135 \cdot 18200 + 701 \cdot 3505 \end{aligned}$$

and so we see $\boxed{5 = -135 \cdot 18200 + 701 \cdot 3505}$ so we can take $x = -135$ and $y = 701$.

(f) $a = 233$, $b = 144$.

- Applying the Euclidean algorithm to $a = 233$ and $b = 144$ yields

$$\begin{aligned} 233 &= 1 \cdot 144 + 89 \\ 144 &= 1 \cdot 89 + 55 \\ 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

and so the gcd is the last nonzero remainder of $\boxed{1}$.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 89 &= & &= 233 - 1 \cdot 144 \\ 55 &= 144 - 1 \cdot 89 &= &= -1 \cdot 233 + 2 \cdot 144 \\ 34 &= 89 - 1 \cdot 55 &= &= 2 \cdot 233 - 3 \cdot 144 \\ 21 &= 55 - 1 \cdot 34 &= &= -3 \cdot 233 + 5 \cdot 144 \\ 13 &= 34 - 1 \cdot 21 &= &= 5 \cdot 233 - 8 \cdot 144 \\ 8 &= 21 - 1 \cdot 13 &= &= -8 \cdot 233 + 13 \cdot 144 \\ 5 &= 13 - 1 \cdot 8 &= &= 13 \cdot 233 - 21 \cdot 144 \\ 3 &= 8 - 1 \cdot 5 &= &= -21 \cdot 233 + 34 \cdot 144 \\ 2 &= 5 - 1 \cdot 3 &= &= 34 \cdot 233 - 55 \cdot 144 \\ 1 &= 3 - 1 \cdot 2 &= &= -55 \cdot 233 + 89 \cdot 144 \end{aligned}$$

and so we see $\boxed{1 = -55 \cdot 233 + 89 \cdot 144}$ so we can take $x = -55$ and $y = 89$.

2. Find the following:

(a) The gcd and lcm of 288 and 600.

- From the Euclidean algorithm we find $\gcd(288, 600) = \boxed{24}$. Then $\text{lcm}(288, 600) = 288 \cdot 600 / 24 = \boxed{7200}$.

(b) The prime factorizations of 2025 and 2026. (You may want to use a calculator for these!)

- Using trial division or a computer we can find $2025 = \boxed{3^4 5^2}$ and $2026 = \boxed{2 \cdot 1013}$.

(c) The prime factorizations of 2025^{2026} and 2026^{2025} .

- Using (b) we see $2025^{2026} = \boxed{3^{8104} 5^{4052}}$ and $2026^{2025} = \boxed{2^{2025} 1013^{2025}}$.

(d) The prime factorizations of 111, 1001, and 111111.

- Using trial division we can find $111 = \boxed{3 \cdot 37}$ and $1001 = \boxed{7 \cdot 11 \cdot 13}$.
- Then $111111 = 111 \cdot 1001 = \boxed{3 \cdot 7 \cdot 11 \cdot 13 \cdot 37}$.

(e) The gcd and lcm of $2^8 3^{11} 5^7 7^8 11^2$ and $2^4 3^8 5^7 7^7 11^{11}$.

- From the prime factorizations, the gcd is $\boxed{2^4 3^8 5^7 7^7 11^2}$ (take the minimum of the two exponents) and the lcm is $\boxed{2^8 3^{11} 5^7 7^8 11^{11}}$ (take the maximum of the two exponents).

(f) The prime factorization of $12!$ and the number of positive divisors of $12!$.

- Noting $12! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$, the primes appearing are 2, 3, 5, 7, 11.
- Counting powers of each prime yields $15! = \boxed{2^{10} 3^5 5^2 7 \cdot 11}$.
- By the number-of-divisors formula, the number of divisors is $(1+10)(1+5)(1+2)(1+1)(1+1) = 11 \cdot 6 \cdot 3 \cdot 2 \cdot 2 = \boxed{792}$.

(g) The number of positive divisors and the sum of positive divisors of 10000.

- Since $10000 = 2^4 5^4$ we see it has $(4+1)(4+1) = \boxed{25}$ divisors, and the sum of divisors is $(1+2+2^2+2^3+2^4)(1+5+5^2+5^3+5^4) = \boxed{24211}$.

3. It is sometimes claimed (occasionally in actual textbooks) that if $p_1, p_2, \dots, p_k$ are the first k primes, then the number $n = p_1 p_2 \cdots p_k + 1$ used in Euclid's proof is always prime for any $k \geq 1$. Find a counterexample to this statement; make sure to justify that it is actually a counterexample.

- Although $2 \cdot 3 + 1 = 7$, $2 \cdot 3 \cdot 5 + 1 = 31$, $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, and $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ are all prime, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ is not, since $30031 = 59 \cdot 509$.

4. Let n be a positive integer greater than 1.

(a) Show that if n is composite, then n must have at least one divisor d with $1 < d \leq \sqrt{n}$. Deduce that if n is composite, then n has at least one *prime* divisor $p \leq \sqrt{n}$. [Hint: Write $n = ab$ where $1 < a \leq b < n$.]

- Since n is composite, we can write $n = ab$ for some $1 < a \leq b < n$.
- Then we see that $a^2 \leq ab = n$, and so $a \leq \sqrt{n}$. Thus, n has a divisor (namely a) that is $\leq \sqrt{n}$ as claimed.
- For the second statement, simply let p be any prime divisor of a : then $1 < p \leq a \leq \sqrt{n}$, and p divides a hence n . Thus, n has a prime divisor $\leq \sqrt{n}$.

(b) Show that if no prime less than or equal to $\sqrt{n}$ divides n , then n is prime.

- This is simply the contrapositive of the second statement in part (a): if n has no prime divisor $p \leq \sqrt{n}$ then n is not composite (i.e., n is prime).

(c) Show explicitly that $n = 109$ and $n = 251$ are prime by verifying that they are not divisible by any prime $\leq \sqrt{n}$.

- Note that $\sqrt{109} < \sqrt{121} = 11$, so for 109 we only have to check the primes 2,3,5,7. But since $109 = 54 \cdot 2 + 1 = 36 \cdot 3 + 1 = 21 \cdot 5 + 4 = 15 \cdot 7 + 4$ we see that none of the primes 2,3,5,7 divide 109, so 109 is prime.
- Likewise, since $\sqrt{251} < \sqrt{256} = 16$, for 251 we only have to check the primes 2,3,5,7,11,13. Since $251 = 2 \cdot 125 + 1 = 3 \cdot 83 + 2 = 50 \cdot 5 + 1 = 35 \cdot 7 + 6 = 22 \cdot 11 + 9 = 19 \cdot 13 + 4$, none of these primes divide 251, so 251 is prime.

5. Recall that the factorial of n is defined as $n! = n \cdot (n-1) \cdots 1$, so for example $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$. (Note that $0!$ is defined to be 1.)

(a) If $n \geq 3$, show that the integers $n! + 2, n! + 3, \dots, n! + n$ are all composite.

- Notice that for any $2 \leq k \leq n$, we have k appearing as a factor in $n!$, and so $n! + k = k \cdot [1 \cdot 2 \cdots (k-1) \cdot (k+1) \cdots n + 1]$.
- Since the term k and the remaining term $1 \cdot 2 \cdots (k-1) \cdot (k+1) \cdots n + 1$ are both greater than 1, this gives an explicit factorization of $n! + k$, so it is composite as claimed.

(b) Suppose we list the primes in increasing order: $p_1 < p_2 < p_3 < \cdots$, so, for instance, $p_5 = 11$. For an arbitrary positive integer n , show that there is some pair of consecutive primes p_k, p_{k+1} such that $p_{k+1} - p_k \geq n$: in other words, that there exists a “prime gap” of size at least n .

- By (a), none of the $n-1$ numbers $n! + 2, n! + 3, \dots, n! + n$ is prime. So if p_k is the largest prime below $n! + 2$ and p_{k+1} is the smallest prime above $n! + n$, then $p_{k+1} - p_k \geq (n! + n + 1) - (n! + 1) = n$, as required.

Remark: Part (b) shows that there are arbitrarily large prime gaps. The smallest possible prime gap that could occur infinitely often is 2, and the twin prime conjecture says that there are infinitely many pairs of consecutive primes that differ by 2.

6. The goal of this problem is to study which numbers of the form $N = a^k - 1$ can be prime, where a and k are positive integers greater than 1.

(a) Show that if $a > 2$, then $N = a^k - 1$ is not prime.

- By factoring, we see $N = a^k - 1$ has $N = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$.
- Since $a > 1$, both factors are greater than 1, so N is composite.

(b) Show that if k is composite, then $N = 2^k - 1$ is not prime. [Hint: If $k = rs$, show N is divisible by $2^r - 1$.]

- By factoring, we see $(2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$.
- Again since $r, s > 1$ we see that both factors are greater than 1, so N is composite.

(c) Deduce that the only possible primes of the form $N = a^k - 1$ are those of the form $2^p - 1$ where p is a prime. (Such primes are called Mersenne primes.) Are all the numbers of the form $2^p - 1$ (p prime) actually prime?

- The first part follows from parts (a) and (b), since $a^k - 1$ is composite if $a \neq 2$ and k is nonprime.
- However, not all numbers of the form $2^p - 1$ with p prime are prime: although $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$ are prime, we have $2^{11} - 1 = 23 \cdot 89$, so $2^p - 1$ is not always prime even when p is prime.

Remark: Mersenne primes can be used to construct perfect numbers, as described in problem 8.

7. Suppose $a|c$ and $b|c$ where a and b are relatively prime. Show that $(ab)|c$.

- Solution 1: Since a divides c , $c = ka$ for some integer k . Then $b|(ka)$ and b is relatively prime to a , so by the relatively prime divisibility property, we see $b|k$ so $k = lb$ for some l . Then $c = ka = l(ab)$ so ab divides c .
- Solution 2: Since a, b are relatively prime there exist integers x and y with $xa + yb = 1$. Multiplying by c yields $xac + ybc = c$, and ab divides both ac (since $b|c$) and ab divides bc (since $a|c$): thus, ab divides c .

Remark: More generally, if $a|c$ and $b|c$ then c is always divisible by $\text{lcm}(a, b)$. (If you want to solve the problem using this fact, you need to prove it!)

8. Recall that if N is a positive integer, then $\sigma(N)$ denotes the sum of the positive divisors of N . We say that N is a perfect number when $\sigma(N) = 2N$: this is often phrased as “the sum of all of the proper divisors of N equals N itself”.

- (a) Show that if $2^{n+1} - 1$ is a prime number, then the number $N = 2^n(2^{n+1} - 1)$ is perfect.
- If $2^{n+1} - 1$ is prime, then by the formula for the sum of divisors, with $N = 2^n(2^{n+1} - 1)$ we have $\sigma(N) = (1 + 2 + \cdots + 2^n)(1 + 2^{n+1} - 1) = (2^{n+1} - 1)2^{n+1} = 2N$, so N is perfect.
- (b) Show that 28, 496, and 8128 are perfect numbers.
- Note that $28 = 2^2 \cdot 7$, $496 = 2^4 \cdot 31$, and $8128 = 2^6 \cdot 127$, so by part (a) since each of $7 = 2^3 - 1$, $31 = 2^5 - 1$, and $127 = 2^7 - 1$ is a prime, we see that 28, 496, and 8128 are perfect numbers.

We would now like to prove a partial converse to (a): namely, that every even perfect number must be of the form given in (a). So suppose $N = 2^n c$ is a perfect number where $n \geq 1$ and c is odd, and observe that $\sigma(N) = (2^{n+1} - 1)\sigma(c)$.

- (c) Show that c must be divisible by $2^{n+1} - 1$.
- Since $\sigma(N) = 2N$ the formula for $\sigma(N)$ gives $2^{n+1}c = (2^{n+1} - 1)\sigma(c)$, so $2^{n+1} - 1$ divides $2^{n+1}c$.
 - But $2^{n+1} - 1$ is relatively prime to 2^{n+1} , so by the relatively prime divisibility property, it must divide the other factor c .
- (d) Show that c must equal $2^{n+1} - 1$ and that $2^{n+1} - 1$ is prime. [Hint: Use $\sigma(c) = 2^{n+1}c/(2^{n+1} - 1)$ and the fact that c has two divisors c and $c/(2^{n+1} - 1)$ to conclude it has no other divisors.]
- By (c) we know that c is divisible by $2^{n+1} - 1$ so c has at least the two divisors c and $c/(2^{n+1} - 1)$.
 - But from (c) we also saw that $\sigma(c) = 2^{n+1}c/(2^{n+1} - 1) = c + c/(2^{n+1} - 1)$, and so these are the only two divisors of c . Therefore, the smaller one $c/(2^{n+1} - 1)$ must be 1, hence $c = 2^{n+1} - 1$, and the larger one $c = 2^{n+1} - 1$ must be prime.
- (e) Deduce that the even perfect numbers are precisely the numbers of the form $N = 2^n(2^{n+1} - 1)$ where $2^{n+1} - 1$ is prime.
- This is immediate from (a) and (d), since (a) showed all these numbers are perfect and (d) shows any even perfect number is of the form $N = 2^n c$ where $c = 2^{n+1} - 1$ is prime.

Remark: Perfect numbers have been of mathematical (and numerological) interest since antiquity. Euclid established the result in (a), and roughly two millennia later, Euler proved the result in (e). It is not known whether there are infinitely many even perfect numbers, and it is also not known whether there are any odd perfect numbers.
