

Tutorial 1

1. In each case find the greatest common divisor of a and b , and integers r, s such that $\gcd(a, b) = ra + sb$.

(i) $a = 35, b = 14$; (ii) $a = 168, b = 132$; (iii) $a = 847, b = 510$.

Solution.

(i)

A	B	35	14	7	0
	Q			2	2
L	K	0	1	2	5
N	M	1	0	1	2.

This table is computed as follows. Firstly, the first two columns of numbers are filled in, using the given values of a and b (namely 35 and 14) as the initial values of A and B , and 0, 1, 1, 0 as the initial values of L, K, N and M (respectively). (If instead of putting $A = 35$ and $B = 14$ you put $A = 14$ and $B = 35$ everything would still work, but it would take one extra step. It makes sense to start by dividing the smaller number into the larger one, rather than vice versa.) Now divide B into A , and put the remainder R into the top row (the new value of B) and the quotient Q underneath it. Underneath Q put $QK + L$ (the new K) and under that put $QM + N$ (the new M). Repeat until $B = 0$. The second last entry in the top row will be the gcd (7 in this case) and the integers r and s that we seek are either the final values of N and $-L$ (if completion occurs after an even number of steps) or the final values of $-N$ and L (for an odd number of steps). In this example we finished in two steps; so r is 1 (the 2nd last number in the last row) and s is -2 (the negative of the 2nd last number in the second last row). We readily check that $1 \times 35 + (-2) \times 14 = 7$.

(ii)

A	B	168	132	36	24	12	0
	Q			1	3	1	2
L	K	0	1	1	4	5	14
N	M	1	0	1	3	4	11.

The gcd is 12, and it took an even number of steps; so $r = 4$ and $s = -5$. We check that

$$4 \times 168 + (-5) \times 132 = 672 - 660 = 12.$$

(iii)

A	B	847	510	337	173	164	9	2	1	0
	Q			1	1	1	1	18	4	2
L	K	0	1	1	2	3	5	93	377	847
N	M	1	0	1	1	2	3	56	227	510.

The gcd is 1, and this time the number of steps was odd; so $r = -227$ and $s = 377$. We check that

$$(-227) \times 847 + 377 \times 510 = -192269 + 192270 = 1.$$

2. (i) Use Fermat's factorization method to factorize 629 and 3139.
 *(ii) Let $n = 10875593$. Aiming to factorize n , I found (with the assistance of MAGMA) that $3306^2 - n = 11 \cdot 17^3$ and $3834^2 - n = 11^3 \cdot 13^2 \cdot 17$. Deduce from this that $(3306 \cdot 3834)^2 - (11^2 \cdot 13 \cdot 17^2)^2$ is divisible by n . Now use a calculator and the Euclidean Algorithm to find a factor of n . What is the smallest a such that $a^2 - n$ is a square?

Solution.

- (i) We find that $25^2 = 625 < 629 < 26^2$. Now
 $26^2 - 629 = 676 - 629 = 47$, not a square.
 $27^2 - 629 = (27^2 - 26^2) + 47 = 53 + 47 = 100$, a square.

So $629 = 27^2 - 10^2 = (27 + 10)(27 - 10) = 37 \times 17$.

We find that $56^2 = 3136 < 3139 < 57^2$. Now

$$57^2 - 3139 = 3249 - 3139 = 110, \text{ not a square.}$$

$$58^2 - 3139 = (58^2 - 57^2) + 110 = 115 + 110 = 225, \text{ a square.}$$

So $3139 = 58^2 - 15^2 = (58 + 15)(58 - 15) = 73 \times 43$.

(ii) See separate solutions sheet.

3. Expand out the product $(x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2)$. Use the result to determine all pairs of integers n, m such that $n^4 + 4m^4$ is prime.

Solution.

$$\begin{aligned} (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2) &= ((x^2 + 2y^2) - 2xy)((x^2 + 2y^2) + 2xy) \\ &= (x^2 + 2y^2)^2 - (2xy)^2 \\ &= x^4 + 4x^2y^2 + 4y^4 - 4x^2y^2 \\ &= x^4 + 4y^4. \end{aligned}$$

Now if n and m are integers then $n^2 - 2nm + 2m^2$ and $n^2 + 2nm + 2m^2$ are both integers, and so the integer $n^4 + 4m^4$ can always be factorized as the product of the two integers $n^2 - 2nm + 2m^2$ and $n^2 + 2nm + 2m^2$. But if a prime number p factorizes as ab (with $a, b \in \mathbb{Z}$) then we must have $a = 1$ and $b = p$ or $a = -1$

and $b = -p$ or $a = p$ and $b = 1$ or $a = -b$ and $p = -1$. So $n^4 + 4m^4$ is definitely not prime unless one of $n^2 - 2nm + 2m^2$ and $n^2 + 2nm + 2m^2$ is equal to ± 1 .

We may as well assume that $n \geq 0$ and $m \geq 0$ since replacing n by $-n$ and/or replacing m by $-m$ does not change the value of $n^4 + 4m^4$. This ensures that $n^2 + 2nm + 2m^2 > n^2 - 2nm + 2m^2$, and by “completing the square” we also see that $n^2 - 2nm + 2m^2 = (n - m)^2 + m^2 \geq 0$. So if $n^4 + 4m^4$ is prime then we must have $(n - m)^2 + m^2 = 1$, which forces $n - m = 0$ and $m = 1$ or $n - m = \pm 1$ and $m = 0$. The latter alternative gives $n = \pm 1$ and $m = 0$, and $n^4 + 4m^4 = 1$, which is not a prime number. The former alternative gives $m = n = 1$, and $n^4 + 4m^4 = 5$, which is prime. The only other solutions correspond to changing the sign of n and/or changing the sign of m . So the only solutions are $n = \pm 1$ and $m = \pm 1$, and 5 is the only prime that can be written as $n^4 + 4m^4$.

4. Let n be a positive integer. The number $n!$ (called “ n factorial”) is defined to be the product of all the positive integers from 1 to n .

(i) Show that if n is composite then $(n - 1)!$ is a multiple of n , unless $n = 4$.

(ii) Show that if n is composite then $(n - 1)! + 1$ is not a multiple of n .

(iii) Compute $(p - 1)! + 1$ for the first five prime numbers p , and check that in each case $(p - 1)! + 1$ is a multiple of p

*(iv) Prove that $(p - 1)! + 1$ is a multiple of p if and only if p is prime.

Solution.

(i) Suppose that n is composite, and write $n = ab$ with $1 < a \leq b < n$. If $b \neq a$ then a and b are distinct factors of $(n - 1)!$; so

$$(n - 1)! = 1 \times \cdots \times a \times \cdots \times b \times \cdots \times (n - 1) = abK = nK$$

where K is the product of all the positive integers less than n , excluding a and b . So $n | (n - 1)!$ in this case.

Suppose instead that $b = a$, so that $n = a^2$. If $2a < n$ then a and $2a$ are distinct factors of $(n - 1)!$; so

$$(n - 1)! = 1 \times \cdots \times a \times \cdots \times 2a \times \cdots \times (n - 1) = 2aK = n(2K)$$

where K is the product of all the positive integers less than n , excluding a and $2a$. So $n | (n - 1)!$ in this case also. So it remains to consider the possibility that $2a \geq n = a^2$. This forces $a \leq 2$, and since we originally assumed that $a > 1$ we must actually have $a = 2$. So the only possible composite number n such that $n \nmid (n - 1)!$ is $n = 2^2 = 4$. (And in this case $(n - 1)! = 6$ is indeed not a multiple of $n = 4$.)

(ii) Let n be composite. By Part (i), $(n - 1)!$ is a multiple of n unless $n = 4$, and so the residue of $(n - 1)! + 1 \pmod n$ is 1. So $(n - 1)! + 1$ is not a multiple

of n in this case. In the remaining case we find that $(n - 1)! + 1 = 7$, which is not a multiple of $n = 4$. So $(n - 1)! + 1$ is never a multiple of n if n is composite.

(iii) The first 5 primes are 2, 3, 5, 7 and 11, and the corresponding values of $(p - 1)! + 1$ are 2, 3, 25, 721 and 3628801. In each case $p | (p - 1)! + 1$. It is in fact true that $p | (p - 1)! + 1$ whenever p is prime; this result is known as *Wilson's Theorem*.

5. Let k be a positive integer and p a prime, and put $n = p^k$. Find a formula for the sum of all the positive integers that are divisors of n . (Hint: the divisors form a geometric progression.)

Solution.

The divisors of p^k are $1, p, p^2, \dots, p^k$, and using the formula

$$a + ar + ar^2 + \cdots + ar^{n-1} = a \frac{(r^n - 1)}{r - 1}$$

we find that the sum of the divisors of p^k is $(p^{k+1} - 1)/(p - 1)$.

*6. (i) Use the formula $1 + x^k + x^{2k} + \cdots + x^{(n-1)k} = \frac{x^{nk} - 1}{x^k - 1}$ to show that if b divides a then $2^b - 1$ divides $2^a - 1$.

(ii) Suppose that $a = qb + r$. Show that $(2^a - 1) - (2^r - 1)$ is a multiple of $2^b - 1$, and hence show that if r is the residue of a modulo b then $2^r - 1$ is the residue of $2^a - 1$ modulo $2^b - 1$.

(iii) Let $a, b, n \in \mathbb{Z}^+$, and let $d = \gcd(a, b)$. Use the Euclidean Algorithm to show that $\gcd(2^a - 1, 2^b - 1) = 2^d - 1$.

Solution.

(i) Let $a = nb$. If we replace x by 2 and k by b then the given formula tells us that

$$(1 + 2^b + 2^{2b} + \cdots + 2^{(n-1)b})(2^b - 1) = (2^{nb} - 1) = 2^a - 1.$$

Thus $2^b - 1 | 2^a - 1$, as required.

(ii) Putting $a = qb + r$ we find that

$$(2^a - 1) - (2^r - 1) = 2^{qb+r} - 2^r = 2^r(2^{qb} - 1) = 2^r N(2^b - 1)$$

for some integer N , by Part (i). Thus

$$2^a - 1 = Q(2^b - 1) + (2^r - 1),$$

where $Q = 2^r N$. If we let q be the quotient and r the remainder on dividing a by b then $0 \leq r < b$ and the equation $a = qb + r$ holds. Clearly $0 \leq r < b$ implies that $0 \leq 2^r - 1 < 2^b - 1$, and since $2^a - 1 = Q(2^b - 1) + (2^r - 1)$ (as shown above) we conclude that $2^r - 1$ is the residue of $2^a - 1$ modulo $2^b - 1$, as desired.