Solution *Section* 2.5 – Primes and Greatest Common Divisors

Exercise

Determine whether each of these integers is prime.

a) 21 *b)* 29 *c)* 71 *d)* 97 *e)* 111
f) 143 *g)* 19 *h)* 27 *i)* 93 *j)* 101
k) 107 *l)* 113

Solution

The numbers: 29, 71, 97, 19, 101, 107, and 113 are primes.

Not Prime: $21 = 3 \cdot 7$ $111 = 3 \cdot 37$ $143 = 13 \cdot 11$ $27 = 3^3$ $93 = 3 \cdot 31$

Exercise

Find the prime factorization of each these integers.

a) 88 *b)* 126 *c)* 729 *d)* 1001 *e)* 1111
f) 909,090 *g)* 39 *h)* 81 *i)* 101 *j)* 143
k) 289 *l)* 899

Solution

a) $88 = 2^3 \cdot 11$

b) $126 = 2 \cdot 3^2 \cdot 7$

c) $729 = 3^6$

d) $1001 = 11 \cdot 91$

e) $1111 = 11 \cdot 101$

f) $909090 = 2 \cdot 5 \cdot 9 \cdot 91 \cdot 111$

g) $39 = 3 \cdot 13$

h) $81 = 3^4$

i) $101 = 101$ (***Prime***)

j) $143 = 11 \cdot 13$

k) $289 = 17^2$

l) $899 = 29 \cdot 31$

Exercise

Find the prime factorization of 10!

Solution

$10! = 3628800$

$10! = (2 \cdot 5)!$

Exercise

Show that if $a^m + 1$ is composite if a and m are integers greater than 1 and m is odd. [*Hint*: Show that $x + 1$ is a factor of the polynomial $a^m + 1$ if m is odd]

Solution

Since m is odd, then we can factor $a^m + 1 = (a+1)\left(a^{m-1} - a^{m-2} + a^{m-3} - \cdots - 1\right)$

Because a and m are both greater than 1, we know that $1 < a + 1 < a^m + 1$. This provides a factoring of $a^m + 1$ into proper factors, so $a^m + 1$ is composite.

Exercise

Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer n. [*Hint*: First show the polynomial identity $x^m + 1 = \left(x^k + 1\right)\left(x^{k(t-1)} - x^{k(t-2)} + \cdots - x^k + 1\right)$ holds, where $m = kt$ and t is odd]

Solution

Assume $y = x^k$, then the claimed identity is

$$\left(y^t + 1\right) = (y+1)\left(y^{t-1} - y^{t-2} + y^{t-3} - \cdots - y + 1\right)$$

By multiplying out the right-hand side and noticing the "telescoping" that occurs.
Let show that m is a power of 2 that is only prime factor is 2.

Suppose to the contrary that m has an odd prime factor t and $m = kt$, where k is a positive integer. Letting $x = 2$ in the identity given in the hint, we have $2^m + 1 = \left(2^k + 1\right)(\cdots)$. Because $2^k + 1 > 1$ and the prime $2^m + 1$ can have no proper factor greater than 1, we must have $2^m + 1 = 2^k + 1$, so $m = k$ and $t = 1$ contradicting the fact that t is prime. This completes the proof by contradiction.

Exercise

Which positive integers less than 12 are relatively prime to 12?

Solution

By inspection with mental arithmetic, the greatest common divisors of the numbers from 1 to 11 with 12 whose ***gcd*** is 1, are 1, 5, 7, and 11. These are so few since 12 had many factors – in particular, both 2 and 3.

Exercise

Which positive integers less than 30 are relatively prime to 30?

Solution

The prime factors of 30 are 2, 3, and 5.

Thus we are looking for positive integers less than 30 that have none of these prime factors. Since the smallest prime number other than these is 7, and 7^2 is already greater than 30, in fact only primes (and the number 1) will satisfy this condition.

Therefore the answer is 1, 7, 11, 13, 17, 18, 23, and 29.

Exercise

Determine whether the integers in each of these sets are pairwise relatively prime.

a) 21, 34, 55 *b)* 14, 17, 85 *c)* 25, 41, 49, 64 *d)* 17, 18, 19, 23

e) 11, 15, 19 *f)* 14, 15, 21 *g)* 12, 17, 31, 37 *h)* 7, 8, 9, 11

Solution

a) $21 = 3 \cdot 7, \quad 34 = 2 \cdot 17, \quad 55 = 5 \cdot 11$ These are pairwise relatively prime

b) $85 = 5 \cdot 17$ These are not pairwise relatively prime

c) $25 = 5^2, \quad 41 \, is \, prime, \quad 49 = 7^2, \quad 64 = 2^6$ These are pairwise relatively prime

d) $17, 19, \, and \, 23 \, are \, prime \quad 18 = 2 \cdot 3^2$ These are pairwise relatively prime

e) $11 \, and \, 19 \, are \, prime \quad 15 = 3 \cdot 5$ These are pairwise relatively prime

f) $14 = 2 \cdot 7 \quad and \quad 21 = 3 \cdot 7$ These are not pairwise relatively prime

g) $17, 31, \, and \, 37 \, are \, prime \quad 12 = 2^2 \cdot 3$ These are pairwise relatively prime

h) $7 \, and \, 11 \, are \, prime \quad 8 = 2^3 \quad 9 = 3^2$ These are pairwise relatively prime

Exercise

We call a positive integer ***perfect*** if it equals the sum of its positive divisors other than itself

a) Show that 6 and 28 are perfect.

b) Show that $2^{p-1}\left(2^p-1\right)$ is a perfect number when 2^p-1 is prime

Solution

a) Since $6=1+2+3$, and these three summands are the only proper divisors of 6, we conclude that 6 is perfect.
$28=1+2+4+7+14$ are also the only proper divisors of 28

b) We need to find all proper divisors of $2^{p-1}\left(2^p-1\right)$. Certainly all the numbers

1, 2, 4, 8, …, 2^{p-1} are proper divisors, and their sum is 2^p-1 (geometric series). Also each of these divisors times 2^p-1 is also a divisor, and all but the last is proper. Again adding up this geometric series we find a sum of $2^{p-1}\left(2^p-1\right)$. There are no other proper divisors.

Therefore the sum of all the divisors is

$$\left(2^p-1\right)+\left(2^p-1\right)\left(2^{p-1}-1\right)=\left(2^p-1\right)\left(1+2^{p-1}-1\right)$$
$$=\left(2^p-1\right)2^{p-1}$$

Which is our original number. Therefore this number is perfect.

Exercise

Show that if 2^n-1 is prime, then *n* is prime. *Hint*: Use the identity

$$2^{ab}-1=\left(2^a-1\right)\cdot\left(2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1\right)$$

Solution

We will prove the assertion by proving its contrapositive.
Suppose that *n* is not prime. Then by definition $n=ab$ for some integers *a* and *b* each greater than 1. Since $a>1$, 2^a-1, the first factor in the suggested identity, is greater than 1. The second factor is also greater than 1.

Thus $2^n-1=2^b-1$ is the product of 2 integers each greater than 1, so it is not prime.

Exercise

Determine whether each of these integers is prime, verifying some of Mersenne's claims

a) $2^7 - 1$ *b)* $2^9 - 1$ *c)* $2^{11} - 1$ *d)* $2^{13} - 1$

Solution

a) $2^7 - 1 = 127$. 2, 3, 5, 7, 11 are not factors of 127, since $\sqrt{127} < 13$, therefore 127 is prime.

b) $2^9 - 1 = 511 = 7 \cdot 73$ So this number is not prime.

c) $2^{11} - 1 = 2047 = 23 \cdot 89$ So this number is not prime.

d) $2^{13} - 1 = 8191$. Since $\sqrt{8191} < 97$ then 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, and 89 are not factors of 8191, therefore 8191 is prime.

Exercise

What are the greatest common divisors of these pairs of integers?

a) $2^2 \cdot 3^3 \cdot 5^5$, $2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) 17, 17^{17}

d) $2^2 \cdot 7$, $5^3 \cdot 13$

e) 0, 5

f) $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) 23^{31}, 23^{17}

j) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$

k) 1111, 0

Solution

a) $2^2 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5$

c) 17

d) 1

e) 5

f) $2 \cdot 3 \cdot 5 \cdot 7$

g) $3^5 \cdot 5^3$

h) 1

i) 23^{17}

j) $41 \cdot 43 \cdot 53$

k) 1111

Exercise

What is the least common multiple of each pair

a) $2^2 \cdot 3^3 \cdot 5^5,\ 2^5 \cdot 3^3 \cdot 5^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13,\ 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

c) $17,\ 17^{17}$

d) $2^2 \cdot 7,\ 5^3 \cdot 13$

e) $0,\ 5$

f) $2 \cdot 3 \cdot 5 \cdot 7,\ 2 \cdot 3 \cdot 5 \cdot 7$

g) $3^7 \cdot 5^3 \cdot 7^3,\ 2^{11} \cdot 3^5 \cdot 5^9$

h) $11 \cdot 13 \cdot 17,\ 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

i) $23^{31},\ 23^{17}$

j) $41 \cdot 43 \cdot 53,\ 41 \cdot 43 \cdot 53$

k) $1111,\ 0$

Solution

a) $2^5 \cdot 3^3 \cdot 5^5$

b) $2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$

c) 17^{17}

d) $2^2 \cdot 5^3 \cdot 7 \cdot 13$

e) *Undefined*

f) $2 \cdot 3 \cdot 5 \cdot 7$

g) $2^{11} \cdot 3^5 \cdot 5^9 \cdot 7^3$

h) $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$

i) 23^{31}

j) $41 \cdot 43 \cdot 53$

k) *Undefined*

Exercise

Find gcd(1000, 625) and lcm(1000, 625) and verify that $\gcd(100,\ 625) \cdot lcm(100,\ 625) = 1000 \cdot 625$

Solution

$1000 = 2^3 \cdot 5^3$

$625 = 5^5$

$\gcd(1000, 625) = 5^3 = 125$

$lcm(1000, 625) = 2^3 \cdot 5^4 = 5000$

Therefore, $125 \cdot 5000 = 625000 = 1000 \cdot 625$

Exercise

Find *gcd*(92928, 123552) and lcm(92928, 123552) and verify that

$gcd\left(92928,\ 123552\right)\cdot lcm\left(92928,\ 123552\right)=92928\bullet 123552$

Solution

$92928=2^8\cdot 3\cdot 11^2$

$123552=2^5\cdot 3^3\cdot 11\cdot 13$

$\gcd\left(92928,\ 123552\right)=2^5\cdot 3\cdot 11=1056$

$lcm\left(92928,\ 123552\right)=2^8\cdot 3^3\cdot 11^2\cdot 13=10{,}872{,}576$

$\gcd\left(92928,\ 123552\right)\cdot lcm\left(92928,\ 123552\right)=\left(2^5\cdot 3\cdot 11\right)\left(2^8\cdot 3^3\cdot 11^2\cdot 13\right)$

$=2^{13}\cdot 3^4\cdot 11^3\cdot 13$

$\left(92928\right)\left(123552\right)=\left(2^8\cdot 3\cdot 11^2\right)\left(2^5\cdot 3^3\cdot 11\cdot 13\right)=2^{13}\cdot 3^4\cdot 11^3\cdot 13$

$\gcd\left(92928,\ 123552\right)\cdot lcm\left(92928,\ 123552\right)=92928\bullet 123552=11{,}481{,}440{,}256$

Exercise

Use the Euclidean algorithm to find

a) $\gcd\left(1,\ 5\right)$ *b)* $\gcd\left(100,\ 101\right)$ *c)* $\gcd\left(123,\ 277\right)$ *d)* $\gcd\left(1529,\ 14039\right)$

e) $\gcd\left(1529,\ 14038\right)$ *f)* $\gcd\left(12,\ 18\right)$ *g)* $\gcd\left(111,\ 201\right)$ *h)* $\gcd\left(1001,\ 1331\right)$

i) $\gcd\left(12345,\ 54321\right)$ *j)* $\gcd\left(1000,\ 5040\right)$ *k)* $\gcd\left(9888,\ 6060\right)$

Solution

a) $5 = 1 \cdot 5 + 0$

$\gcd\left(1,5\right)=\gcd\left(1,0\right)=1$

b) $101 = 100 \cdot 1 + 1$

$1 = 1 \cdot 1 + 0$

$\gcd\left(100,101\right)=\gcd\left(100,1\right)=\gcd\left(1,0\right)=1$

c) $277 = 123 \cdot 2 + 31$

$123 = 31 \cdot 3 + 30$

$31 = 30 \cdot 1 + 1$

$30 = 1 \cdot 30 + 0$

$\gcd\left(123,\ 277\right)=\gcd\left(123,31\right)=\gcd\left(31,30\right)=\gcd\left(30,1\right)=\gcd\left(1,0\right)=1$

d) $14039 = 1529 \cdot 9 + 278$

$1529 = 278 \cdot 5 + 139$

$278 = 139 \cdot 2 + 0$

$\gcd\left(1529,\ 14039\right)=\gcd\left(1529,\ 278\right)=\gcd\left(278,\ 139\right)=\gcd\left(139,\ 0\right)=139$

e) $14038 = 1529 \cdot 9 + 277$
$1529 = 277 \cdot 5 + 144$
$277 = 144 \cdot 1 + 133$
$144 = 133 \cdot 1 + 11$
$133 = 11 \cdot 12 + 1$
$11 = 1 \cdot 11 + 0$
$\gcd(1529, 14038) = \gcd(1529, 277) = \gcd(277, 144) = \gcd(144, 133) = \gcd(133, 11)$
$= \gcd(11, 1) = \gcd(1, 0) = 1$

f) $18 = 12 \cdot 1 + 6$
$12 = 6 \cdot 2 + 0$
$\gcd(12,18) = \gcd(12, 6) = 6$

g) $201 = 111 \cdot 1 + 90$
$111 = 90 \cdot 1 + 21$
$90 = 21 \cdot 4 + 6$
$21 = 6 \cdot 3 + 3$
$6 = 3 \cdot 2 + 0$
$\gcd(111,201) = \gcd(111,90) = \gcd(90,21) = \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = 3$

h) $1331 = 1001 \cdot 1 + 330$
$1001 = 330 \cdot 3 + 11$
$330 = 11 \cdot 30 + 0$
$\gcd(1001,1331) = \gcd(1001,330) = \gcd(330,11) = \gcd(11,0) = 11$

i) $54321 = 12345 \cdot 4 + 4941$
$12345 = 4941 \cdot 2 + 2463$
$4941 = 2463 \cdot 2 + 15$
$2463 = 15 \cdot 164 + 3$
$15 = 3 \cdot 5 + 0$
$\gcd(12345, 54321) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463, 15)$
$= \gcd(15, 3) = \gcd(3, 0) = 3$

j) $5040 = 1000 \cdot 5 + 40$
$1000 = 40 \cdot 25 + 0$
$\gcd(1000, 5040) = \gcd(1000, 40) = \gcd(40, 0) = 40$

k) $9888 = 6060 \cdot 1 + 3828$
$6060 = 3828 \cdot 1 + 2232$
$3828 = 2232 \cdot 1 + 1596$
$2232 = 1596 \cdot 1 + 636$
$1596 = 636 \cdot 2 + 324$
$636 = 324 \cdot 1 + 312$
$324 = 312 \cdot 1 + 12$
$312 = 12 \cdot 26 + 0$
$\gcd(9888, 6060) = \gcd(6060, 3828) = \gcd(3828, 2232) = \gcd(2232, 1596) = \gcd(1596, 636)$
$= \gcd(636, 324) = \gcd(324, 312) = \gcd(312, 12) = \gcd(12, 0) = 12$

Exercise

Prove that the product of any three consecutive integers is divisible by 6.

Solution

Consider the product $n(n+1)(n+2)$ for some integer *n*.

Since every second integer is even (divisible by 2), then this product is divisible by 2.
Since every third integer is divisible by 3, then this product is divisible by 3.
Therefore this product has both 2 and 3 in its prime factorization and is therefore divisible by $2 \cdot 3 = 6$

Exercise

Show that if *a*, *b*, and *m* are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then $\gcd(a,\ m) = \gcd(b,\ m)$

Solution

From $a \equiv b \pmod{m}$ we know that $b = a + sm$ for some integer *s*. If *d* is a common divisor of *a* and *m*, then it divides the right-hand side of this equation, so it also divides *b*. We can rewrite the equation as $a = b - sm$, and they by similar reasoning, we see that every common divisor of *b* and *m* is also a divisor of *a*.
This shows that the set of common divisors of *a* and *m* is equal to the set of common divisors of *b* and *m*, so certainly $\gcd(a, m) = \gcd(b, m)$

Exercise

Prove or disprove that $n^2 - 79n + 1601$ is prime whenever *n* is a positive integer.

Solution

Using calculator or spread sheet because it is hard to get started:

All the values are prime. This may lead us to believe that the propositions is true, but it gives no clue as to how to prove it.
If we let *n* = 1601, then
$1601^2 - 79(1601) + 1601 = 1601(1601 - 79 + 1) = 1601 \cdot 1523$.
So we got a counterexample and the proposition is false.

The smallest *n* for which this expression is not prime is *n* = 80; this gives the value $1681 = 41 \cdot 41$

$n^2 - 79n + 1601$	
$n = 1$	1523
$n = 2$	1447
$n = 3$	1373
$n = 4$	1301
$n = 5$	1231
$n = 6$	1163