Anze Wang ID: 912777492
ECS 020 A04

Homework 7

Exercise 1: .

e)-2002 is divided by 89?

$\because -2002 \ mod \ 89 = 45$

$\therefore$ -2002 is not divided by 89

f) 0 is divided by 19?

$\because 0 \ mod \ 19 = 0$

$\therefore$ 0 is divided by 19

g) 1,234,567 is divided by 101?

$\because 1234567 \ mod \ 19 = 14$

$\therefore$ 1,234,567 is not divided by 19

h)-100 is divided by 103?

$\because -100 \ mod \ 103 = 3$

$\therefore$ -100 is not divided by 103

Exercise 2: .

a) Let a be a positive integer. Show that $gcd(a, a-1) = 1$

$$\begin{aligned} &gcd(a, a-1) \\ =&gcd(a-1, 1) \\ =&1 \end{aligned}$$

b) Use the result of part a) to solve the Diophantin eequation

$$a + 2b = 2ab$$

where (a, b) are positive integers

$$\begin{aligned} &a + 2b = 2ab \\ &a = 2(a-1)b \\ &b = \frac{a}{2(a-1)} \end{aligned}$$

Because both a and b are positive integer, we can only get one set of solution, a = 2, b = 1.

Anze Wang ID: 912777492
ECS 020 A04

Exercise 3: .

Leta, b, and c be three integers. Show that the equation $ax + by = c$ has at least one solution (x_1, y_1) if and only if $gcd(a, b) \mid c$

Let p be the proposition "$ax + by = c$ has at least one integer solution (x_1, y_1)" and q be the proposition "$gcd(a, b)/c$". We want to show that $p \leftrightarrow q$, which is logically equivalent to show that $p \leftarrow q$ and $q \rightarrow p$.

i) Let us show $p \rightarrow q$:

Hypothesis: p is true, If $ax + by = c$ has one integer solution (x_1, y_1), then let $a = pd$, $b = qd$ where $d = gcd(a, b)$ and p,q are also integers. We get:

$$\begin{aligned}
&ax + by = c \\
&pdx + qdy = c \\
&d(px + qy) = c
\end{aligned}$$

Because $px + qy$ and c are integers, we can get that $gcd(a, b) \mid c$

ii) Let us show $q \rightarrow p$:

Hypothesis: q is true. If $gcd(a, b) \mid c$, then $c = kgcd(a, b)$, $k \in \mathbb{Z}$. And according to the BZOUTS THEOREM, $gcd(a, b) = sa + tb$, $(a, b) \in \mathbb{Z}^2$ we can get that:

$$\begin{aligned}
c &= k\ gcd(a, b) \\
&= a \cdot sk + b \cdot tk
\end{aligned}$$

So we can get one solution easily:

$$\begin{cases} x = sk \\ y = tk \end{cases}$$

Thus this equation has at least one integer solution when $gcd(a, b) \mid c$

we can conclude that the equation $ax + by = c$ has at least one solution (x_1, y_1) if and only if $gcd(a, b) \mid c$

Exercise 4: .

Let a, b and n be three positive integers with $gcd(a, n) = 1$ and $gcd(b, n) = 1$. Show that $gcd(ab, n) = 1$.

Because $gcd(a, n) = 1$, a and n are relative prime.

So $a = pn + i$, $p \in \mathbb{R}$, $i \in \mathbb{N}, i < n$, i and n are relative prime.

Similarly, we can get $b = qn + j$, $q \in \mathbb{R}$ and $j \in \mathbb{N}, j < n$, i and n are relative prime.

Then $ab = pqn^2 + pjn + qin + ij$

Thus:

$$\begin{aligned}
gcd(ab, n) &= gcd(n, ab\ mod\ n) \\
&= gcd(n, (pqn^2 + pjn + qin + ij)\ mod\ n) \\
&= gcd(n, ij\ mod\ n)
\end{aligned}$$

Because i, n are relative prime and j, n are relative prime, ij and n are relative prime. Therefore, $ij\ mod\ n$ and n are relative prime.

$$gcd(n, ij\ mod\ n) = gcd(ab, n) = 1$$

Exercise 5: .

Prove that there are no solutions in integers x and y to the equation $3x^2 + 5y^2 = 19$.

Let both side mod 3:

$$\begin{aligned} &RHS\ mod\ 3 \\ =&19\ mod\ 3 \\ =&1 \end{aligned}$$

$$\begin{aligned} &LHS\ mod\ 3 \\ =&(3x^2 + 5y^2)\ mod\ 3 \\ =&5y^2\ mod\ 3 \end{aligned}$$

if $y = 1$, $5y^2\ mod\ 3 = 2$

if $y = 2$ $5y^2 = 20 > 19$

So we can conclude that this equation cannot have integer solution.

Exercise 6: .

Show that if $n > 3$ then n, $2n + 1$ and $4n + 1$ cannot all be prime

if $n\ mod\ 3 = 0$: n is not prime.

if $n\ mod\ 3 = 1$, then $n = 3k + 1$, $k \in \mathbb{Z}$, then $2n + 1 = 6k + 3$, which is not prime.

if $n\ mod\ 3 = 2$, then $n = 3k + 2$, $k \in \mathbb{Z}$, then $4n + 1 = 12k + 9$, which is not prime.

Exercise 7: .

Prove or disprove that there are three consecutive odd positive integers that are primes,that is, odd primes of the form p, $p + 2$, $p + 4$.

Because 3, 5, 7 are consecutive odd positive primes, this statement is true.

Exercise 8: .

Prove that if n is a positive integer such that the sum of its divisors is $n + 1$, then n is prime.

let's assume that the sum of its divisors is $n + 1$, and n is not a prime.

Because n is not a prime, $n = 1 * p * q$, $(p, q) \in \mathbb{Z}^+$

Because m,n may not be prime, the sum of n's divisors must greater than or equal to $1 + p + q + n$, which is greater than $n + 1$. This is contradict with my assumption. So we can conclude that if n is a positive integer such that the sum of its divisors is $n + 1$, then n is prime.

Exercise 9: Extra Credit

Let a and b be two strictly positive integers. Solve $gcd(a, b) + lcm(a, b) = b + 9$

Let $a = pd$, $b = qd$,which p, q, d are positive integers

$$\begin{aligned} &gcd(a, b) + lcm(a, b) = b + 9 \\ &d + \frac{pqd^2}{d} = qd + 9 \\ &d + pqd - qd = 9 \\ &d(1 - q + pq) = 9 \end{aligned}$$

Because p ,q ,d are positive integers, we can get these solutions:

$$\begin{cases} d = 3 \\ p = 3 \\ q = 1 \end{cases} \quad \begin{cases} d = 1 \\ p = 3 \\ q = 4 \end{cases} \quad \begin{cases} d = 1 \\ p = 9 \\ q = 1 \end{cases} \quad \begin{cases} d = 1 \\ p = 5 \\ q = 2 \end{cases} \quad \begin{cases} d = 9 \\ p = 1 \\ q = n, n \in \mathbb{Z}, n > 1 \end{cases}$$

So we can know that $(9, 3)$, $(3, 4)$,$(9, 1)$, $(5, 2)$ or $(9, 9n)$