01017/01019 Discrete Mathematics E24
Home assignment 2

Fedir Vasyliev s234542
William Carlsen s223818

13/10/2024

1 Exercise A

1.1

I will prove that the statement if $a \mid bc$ where a, b, c $\in \mathbb{Z}$ and a$\neq$ 0, then $a \mid b$ or $a \mid c$, is false by giving a counterexample. Take for example $a = 8, b = 4, c = 2$, then $a \mid bc$ because $8 \mid 4 \cdot 2$, but $a \nmid b$ and $a \nmid c$ because $8 \nmid 4$ and $8 \nmid 2$. Because there exist an example that makes the statement false, the statement has been disproved.

1.2

To prove the statement if $a \in \mathbb{Z}$, then 5 does not divide $a^2 + 2$, I have to prove that a squared never ends with either a 2 or 7, that is $a^2 \not\equiv 2 \textbf{ mod } 5$. I will prove that by showing that the last digit in a squared integer only depends on the last digit in the integer itself, and then showing that it will never be 2 or 7.

For every $n \in \mathbb{Z}$, n can be written as $n = 10k + b$ where $k \in \mathbb{Z}$ and $b \in \{0, 1, 2, 3..., 9\}$. Then n squared can be written as $n^2 = (10k + b)^2 = 100k^2 + 20kb + b^2$. Since the first two terms is a multiple of 10, they will alwas end with at least one zero. So the last digit is only determined by the factor b^2, whose values are shown below

$1^2 = 1$	$2^2 = 4$	$3^2 = 9$	$4^2 = 16$	$5^2 = 25$
$6^2 = 36$	$7^2 = 49$	$8^2 = 64$	$9^2 = 81$	$0^2 = 0$

Since non of them ends with a 2 or 7, it has been proved that 5 does not divide $a^2 + 2$, when a is an integer.

2 Exercise B

Prove that $n^2 \equiv 1 \, mod \, 8$, where n is positive odd integer.
Let $n = 2k + 1$, $k \in \mathbb{Z}^+$. Thus, from the definition of congruence we can

write

$$(2k+1)^2 - 1 = l \cdot 8,\ \ l \in \mathbb{Z}^+$$

$$\frac{4k^2 + 4k}{8} = l$$

$$\frac{k(k+1)}{2} = l$$

Now we need to prove that $k(k+1)$ is in fact divisible by 2. As k is a positive integer $\Rightarrow$ k and $k+1$ are two consecutive integers, which implies that one of them is even and the other one is odd. The product of an odd and even integer will always be even, and therefore $k(k+1)$ is divisible by 2.

3 Exercise C

Exercise 32
a) $gcd(1, 5) = 1$

b) $gcd(100, 101) = 1$

$$101 = 1 \cdot 100 + 1$$
$$100 = 100 \cdot 1 + 0$$

c)$gcd(123, 277) = 1$

$$277 = 2 \cdot 123 + 31$$
$$123 = 3 \cdot 31 + 30$$
$$31 = 1 \cdot 30 + 1$$
$$30 = 30 \cdot 1 + 0$$

d)$gcd(1529, 14039) = 139$

$$14039 = 9 \cdot 1529 + 278$$
$$1529 = 5 \cdot 278 + 139$$
$$278 = 2 \cdot 139 + 0$$

e)$gcd(1529, 14038) = 1$

$$14038 = 9 \cdot 1529 + 277$$
$$1529 = 5 \cdot 277 + 134$$
$$277 = 2 \cdot 134 + 9$$
$$134 = 14 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1$$
$$8 = 8 \cdot 1 + 0$$

f)$gcd(11111, 111111) = 1$

$$111111 = 10 \cdot 11111 + 1$$
$$11111 = 11111 \cdot 1 + 0$$

Exercise 44
$gcd(1001, 100001) = 11$

$$100001 = 99 \cdot 1001 + 902$$
$$1001 = 1 \cdot 902 + 99$$
$$902 = 9 \cdot 99 + 11$$
$$99 = 9 \cdot 11 + 0$$

$$11 = 902 - 9 \cdot 11$$
$$11 = 902 - 9(1001 - 902) = 10 \cdot 902 - 9 \cdot 1001$$
$$11 = 10(100001 - 99 \cdot 1001) - 9 \cdot 1001$$
$$11 = 10 \cdot 100001 - 999 \cdot 1001$$

4 Exercise D

I will show that an inverse of a modulo m, where a is an integer and m $>$ 2 is a positive integer, does not exist if gcd(a, m)>1

If a has an inverse so $a\overline{a} \equiv 1$ **mod** m, then there is a k such that

$$a\overline{a} = km + 1 \tag{1}$$

since gcd(a, m) divideds both a and m, it also divides any linear combination of a and m. But since gcd(a, m)>1, it does not divide 1, and therefore the equation is a contradiction and an inverse of a does not exist when gcd(a, m)>1.

5 Exercise E

1)

$$x \equiv 1\, mod\, 3$$
$$x \equiv 3\, mod\, 4$$
$$x \equiv 2\, mod\, 5$$
$$m = 3 \cdot 4 \cdot 5 = 60$$
$$M_1 = 20,\ M_2 = 15,\ M_3 = 12$$
$$y_1 = 2,\ y_2 = 3,\ y_3 = 3$$
$$x \equiv 2 \cdot 20 \cdot 1 + 3 \cdot 3 \cdot 15 + 2 \cdot 3 \cdot 12\, mod\, 60$$
$$x \equiv 40 + 135 + 72\, mod\, 60$$
$$x \equiv 247\, mod\, 60$$
$$x \equiv 7\, mod\, 60$$

So $x \in \{7, 67, 127, ...\}$.
2)

$$x \equiv 2 \, mod \, 6$$
$$x \equiv 3 \, mod \, 7$$
$$x = 6t + 2$$
$$6t + 2 \equiv 3 \, mod \, 7$$
$$6t \equiv 1 \, mod \, 7 \, \text{inverse of } 6 \, mod \text{ is} 6$$
$$t \equiv 6 \, mod \, 7$$
$$7v + 6 = t$$
$$x = 6(7v + 6) + 2 = 42v + 38$$
$$x \equiv 38 \, mod \, 42$$

$x \in \{38, 80, ...\}$.