yohandi 120040025
CSC3001 Assignment 3

Q1. 1) let a_n be the number of bit strings of length n that contain 3 consecutive 0's, we consider:

if the string ends with 1,
we can assume that the combinations of length $n-1$ are valid, which is a_{n-1}

if the string ends with 10,
we can assume that the combinations of length $n-2$ are valid, which is a_{n-2}

if the string ends with 100,
we can assume that the combinations of length $n-3$ are valid, which is a_{n-3}

if the string ends with 000,
there are 2^{n-3} possible combinations to construct the valid string of length n-3

$\therefore a_n = a_{n-1} + a_{n-2} + a_{n-3} + 2^{n-3}$

2) we notice that it is impossible to construct a bit string that contains 000 with length < 3. therefore,
$a_0 = a_1 = a_2 = 0$.
$a_3 = a_2 + a_1 + a_0 + 2^0 = 1$ which is true as "000" is the only valid string. hence, a_3 is not the initial value

3) $a_0 = 0$
$a_1 = 0$
$a_2 = 0$
$a_3 = 0+0+0+2^0 = 1$
$a_4 = 1+0+0+2^1 = 3$
$a_5 = 3+1+0+2^2 = 8$
$a_6 = 8+3+1+2^3 = 20$
$a_7 = 20+8+3+2^4 = 47$
hence, 47 bit strings of length 7 are valid

Q2. let $f(x) = \sum_{n=0}^{\infty} a_n x^n$

$\Rightarrow a_n = a_{n-1} + 6a_{n-2}$

$\Rightarrow \sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} (a_{n-1} + 6a_{n-2}) x^n$

$\Rightarrow \sum_{n=0}^{\infty} a_n x^n - a_1x^1 - a_0x^0 = \sum_{n=1}^{\infty} a_n x^{n+1} + \sum_{n=0}^{\infty} 6a_n x^{n+2}$

$\Rightarrow f(x) - 6x - 3 = x(f(x) - 3) + 6x^2 f(x)$

$\Rightarrow f(x)(1 - x - 6x^2) = 3x + 3$

$\Rightarrow f(x) = \dfrac{3x+3}{1-x-6x^2}$

$= \dfrac{12}{5(1-3x)} + \dfrac{3}{5(1+2x)}$

$= \sum_{n=0}^{\infty} \frac{12}{5} \cdot 3^n x^n + \sum_{n=0}^{\infty} \frac{3}{5}(-2)^n x^n$

$= \sum_{n=0}^{\infty} \underbrace{\left(\frac{12}{5} \cdot 3^n + \frac{3}{5}(-2)^n\right)}_{a_n} x^n$

$\therefore a_n = \left(\frac{12}{5} \cdot 3^n + \frac{3}{5}(-2)^n\right)$

Q3. $n^2 \equiv (n \bmod 4)^2 \pmod 4$
since $n \bmod 4 \in \{0,1,2,3\}$, we only need to prove for 0, 1, 2, and 3.

$\Rightarrow$ case $n=0$,
$0^2 \equiv 0 \pmod 4$ (true)

$\Rightarrow$ case $n=1$,
$1^2 \equiv 1 \pmod 4$ (true)

$\Rightarrow$ case $n=2$,
$2^2 = 4 \equiv 0 \pmod 4$ (true)

$\Rightarrow$ case $n=3$
$3^2 = 9 \equiv 1 \pmod 4$ (true)

hence, it is true for n is integer

Q4. $7^{14} = 49^7 \equiv (49 \bmod 47)^7 \pmod{47}$

$= 2^7 \pmod{47}$

$= 128 \pmod{47}$

$= (2 \cdot 47 + 34) \pmod{47}$

$\equiv 34 \pmod{47}$

Q5. If x is an integer solution, then there exists some $y \in \mathbb{Z}$ s.t.

$$5x = 12 + 23y$$

$\Rightarrow 5x - 23y = 12$

by Euclid's division lemma,

$$23 = 5 \cdot 4 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 1 \cdot 1 + 0$$

$\cdot\!> 1 = 3 - 2 = 3 - (5-3) = 3 - 5 + 3 = 2 \cdot 3 - 5$

$= 2(23 - 5 \cdot 4) - 5 = 2 \cdot 23 - 5 \cdot 8 - 5 = 2 \cdot 23 - 5 \cdot 9$

$\Rightarrow 5(-9) - 23(2) = 1$

$\Rightarrow 5(-108) - 23(24) = 12$

Since $-108 \bmod 23 = 7$,

the solution is $(7, 24)$

Q6. we have

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 4$

$x \equiv 1 \pmod 5$

since $\gcd(3,4) = \gcd(4,5) = \gcd(3,5) = 1$, the system has a simultaneous solution which is unique, $\bmod (3 \cdot 4 \cdot 5) = \bmod 60$.

$\cdot\!> 3 \mid x-2 \Rightarrow x = 3t+2,\ t \in \mathbb{Z}$

$\Rightarrow 3t + 2 \equiv 3 \pmod 4$

$\Rightarrow 3t \equiv 1 \pmod 4$

$\Rightarrow t \equiv 3 \pmod 4$

$\cdot\!> 4 \mid t-3$

$\Rightarrow x = 3t + 2$

$\Rightarrow x = 2 + 3(3 + 4s) = 11 + 12s$

$\cdot\!> 11 + 12s \equiv 1 \pmod 5$

$\Rightarrow 2s \equiv 0 \pmod 5$

$\Rightarrow s \equiv 0 \pmod 5$

$\Rightarrow 5 \mid z$

$\cdot\!> x = 11 + 12(5r) = \boxed{11 + 60r,\ r \in \mathbb{Z}}$

$\Rightarrow x \equiv 11 \pmod{60}$

Q7. factorize $n^7 - n$, we obtain:

$$n(n-1)(n^2+n+1)(n+1)(n^2-n+1)$$

proof that $2 \mid n^7 - n$:

n and $n-1$ are two consecutive integers, which shows that one of them is divisible by 2

proof that $3 \mid n^7 - n$:

$n-1$, n, and $n+1$ are three consecutive integers, which shows that one of them is divisible by 2

proof that $7 \mid n^7 - n$:

by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod p$ if p is prime and a is not divisible by p.

$\cdot\!> n^6 = n^{7-1} \equiv 1 \pmod 7$

$\Rightarrow 7 \mid n^6 - 1$

$\cdot\!> n^7 - n = n(n^6 - 1)$

$\Rightarrow 7 \mid n^7 - n$

since $n^7 - n$ is divisible by 2, 3, and 7, $n^7 - n$ is divisible by $\operatorname{lcm}(2,3,7) = 42$

Q8. assume that there are only finite numbers of prime, then we can write those numbers in an array:

$$p_1 \ p_2 \ p_3 \ \cdots \ p_n$$

where n is some finite integer.

let $a = \prod_{i=1}^{n} p_i + 1$, according to the Fundamental Theorem of Arithmetic, there are only 2 possibilities:

(1) a is prime:

this contradicts with our assumption as we can take a as p_{n+1}

(2) a is composite:

a doesn't divide $p_1, p_2, \ldots, p_n$ as it requires unique factorization which violates the Fundamental Theorem of Arithmetic

we reach contradiction which implies there are infinitely many numbers of prime

Q9. $spc(252,198) = \min\{252x+198y \mid 252x+198y>0,\ x,y \in \mathbb{N}\}$

$= 18 \min\{14x+11y \mid 14x+11y>0,\ x,y \in \mathbb{N}\}$

when $x=4$ & $y=-5$, $14x+11y=1$ (which is the smallest positive integer)

$= 18 \cdot 1$

$= 18$

Q10. Since $a \equiv b \pmod m$, there exist integer c s.t. $a = mc+b$.

let $p = \gcd(a,m)$ and $q = \gcd(b,m)$, we have:

$p \mid a$

$p \mid m$

$q \mid b$

$q \mid m$

- $a = mc+b \Rightarrow p \mid b$
- $a = mc+b \Rightarrow q \mid a$

Since $p \mid b$ and $p \mid m$, $p \mid \gcd(b,m)$.

similarly, $q \mid a$ and $q \mid m$, $q \mid \gcd(a,m)$.

$\Rightarrow p \mid q$ and $q \mid p$

$\Rightarrow p = q$

$\Rightarrow \gcd(a,m) = \gcd(b,m)$