Homework 4 Exercises

4.1 Exercises ~~10, 15, 16, 21, 26, 34, 35, 38~~

10. a) 44=8*5+4
    b) 777=21*37+0
    c) -123=19*(-7)+10
    d) -1=23*(-1)+22
    e) -2002=87*(-24)+86
    f) 0=17*0+0
    g) 1234567=1001*1233+334
    h) -100=101*(-1)+1

15. Since a **mod** m = b **mod** m, a and b have the same remainder, suppose $a = t*m+r$, $b = u*m+r$, r denotes the remainder.
    $a - b = t*m+r - (u*m+r) = m(t-u)$
    Since, $m(t-u) / m = t-u$ and $t-u$ is an integer,
    $m(t-u)$ can be divided by m, which means $a - b$ can be divided by m.
    Thus, according to **DEFINITION 3**, we can say $a \equiv b \pmod m$ if a **mod** m = b **mod** m.

16. Since $a \equiv b$ (**mod** m), we can conclude that m can divides $a - b$.
    Suppose $a - b = v*m$, and $a = t*m+r$ (a **mod** $m = r$).
    Here v and t denotes quotients and r denotes remainder.
    Then, $t*m+r - b = v*m$
    $b = t*m+r-v*m$
    $b = (t-v)*m+r$
    We can express this function as b **mod** $m = r$. Because a **mod** $m = r$, a **mod** $m = b$ **mod** m.
    Thus a **mod** $m = b$ **mod** m if $a \equiv b$ (**mod** m).

21. a) 13 **mod** 3 = 1
    b) -97 **mod** 11 = 2
    c) 155 **mod** 19 = 3
    d) -221 **mod** 23 = 9

26. 16, 28, 40, 64, 76. (numbers that can be divided by 12: 16-4=12, 28-4=24, 40-4=36, 64-4=60, 76-4=72)

34. Since $a \equiv b$ (**mod** m) and $c \equiv d$ (**mod** m), we can suppose $a - b = t*m$ and $c-d = u*m$.
    Then $(a-c)-(b-d) = a-c-b+d = a-b-c+d = (a-b)-(c-d) = t*m - u*m = (t-u)*m$
    We can conclude that $(a-c) \equiv (b-d)$ (**mod** m).

35. Since $n \mid m$, we suppose that $m = n*q$ (q denotes the quotient).
    And because $a \equiv b$ (**mod** m), we can suppose that $a-b=m*p$ (p denotes the quotient).
    Then, $a-b = n*q*p$, where p and q are integers because $m \mid a-b$ = p and $n \mid m$ = q.
    Since p and q are integers and $a-b = n*q*p$, we can conclude that $n \mid a-b$,
    which means $a \equiv b$ (**mod** n).

38. If n is an even integer, we can suppose $n = 2k$.
    Then n^2 **mod** 4 = $(2k)^2$ **mod** 4 = $4k^2$ **mod** 4 = 0. Since 0 **mod** 4 = 0 and n^2 **mod** 4 = 0 if n is an even integer, $n \equiv 0$(**mod** 4).
    If n is an odd integer, we can suppose $n = 2k+1$.
    n^2 **mod** 4 = $(2k+1)^2$ **mod** 4 = $4k^2+1+4k$ **mod** 4 =

Based on the previous prove that n is an even integer,

(($4k^2$ **mod** 4) + (1 **mod** 4) + ($4k$ **mod** 4)) **mod** 4 = (0 + 1 + 0) **mod** 4 = 1 **mod** 4 = 1

Since 1 **mod** 4 = 1 and n^2 **mod** 4 = 1 if n is an odd integer, $n \equiv 1$(**mod** 4).

Therefore, based on the prove of the even n and odd n, $n^2 \equiv 0$ or 1 (**mod** 4).

4.3 Exercises ~~2, 3, 15, 21, 22, 28, 33, 38, 50, 54~~

2. 19, 101, 107, and 113 are the prime numbers; 27 and 93 are not prime.

3. a) 88 = 2*2*2*11

b) 126 = 2*7*3*3

c) 729 = 3*3*3*3*3*3

d) 1001 = 7*13*11

e) 1111 = 11*101

f) 909090 = 3*3*2*5*7*13*3*37

15. The integers are 1, 7, 11, 13, 17, 19, 23, 29.

gcd(1, 30) = 1, gcd(7, 30) = 1, gcd(11, 30) = 1, gcd(13, 30) = 1, gcd(17, 30) = 1, gcd(19, 30) = 1, gcd(23, 30) = 1, gcd(29, 30) = 1.

21. a) $\varnothing$ (4) = 2 (1,3)

b) $\varnothing$ (10) = 4 (1, 3, 7, 9)

c) $\varnothing$ (13) = 12 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)

22. 1) If n is prime, then its positive factors are only 1 and n itself. Thus, all positive integers less than n has no common factors, except 1, with n:

gcd (1, n) = 1, gcd (2, n) = 1, gcd (3, n) = 1 ... gcd (1, n-1) = 1.

Thus all positive integers less than n are relatively prime to n.

By the definition of the Euler $\varnothing$ -function, all positive integers less than n are relatively prime to n, thus the value of $\varnothing$ (n) = n-1.

2) If $\varnothing$ (n)=n-1, the numbers of positive integers less than n that are relatively prime to n is n-1, which means there has (n-1) integers that are relatively prime to n, that is, the positive integers less than n does not share any common factors, except 1, with n:

gcd (1, n) = 1, gcd (2, n) = 1, gcd (3, n) = 1 ... gcd (1, n-1) = 1.

Suppose n is composite, then n must have a prime divisor less than or equal to $\sqrt{n}$.

The prime divisor is a factor of n. But all numbers less than n has no common factors, except 1, with n, then n is not a composite number but a prime number.

Based on the conclusions in 1) and 2), therefore, n is prime iff $\varnothing$ (n) = n-1.

28. gcd (1000, 625) = 125

1000 **mod** 625 = 375

625 **mod** 375 = 250

375 **mod** 250 = 125

250 **mod** 125 = 0

lcm (1000,625) = 5000

1000 = 2*2*2*5*5*5

625 = 5*5*5*5

lcm (2*2*2*5*5*5*5)

∴ gcd (1000, 625) * lcm (1000,625) = 125 * 5000 = 625000 = 1000 * 625

33. a) gcd (12, 18)

18 = 12 * 1 + 6

12 = 6 * 2

Hence, gcd (12, 18) = 6.

b) gcd (111, 201)

201 = 111 * 1 + 90

111 = 90 * 1 + 21

90 = 21 * 4 + 6

21 = 6 * 3 + 3

6 = 3 * 2

Hence, gcd (111, 201) = 3.

c) gcd (1001, 1331)

1331 = 1001 * 1 + 330

1001 = 330 * 3 + 11

330 = 11 * 30

Hence, gcd (111, 201) = 11.

d) gcd (12345, 54321)

54321 = 12345 * 4 + 4941

12345 = 4941 * 2 + 2463

4941 = 2463 * 2 + 15

2463 = 15 * 164 + 3

15 = 3 * 5

Hence, gcd (12345, 54321) = 3.

e) gcd (1000, 5040)

5040 = 1000 * 5 + 40

1000 = 40 * 25

Hence, gcd (1000, 5040) = 40.

f) gcd (9888, 6060)

9888 = 6060 * 1 + 3828

6060 = 3828 * 1 + 2232

3828 = 2232 * 1 + 1596

2232 = 1596 * 1 + 636

1596 = 636 * 2 + 324

636 = 324 * 1 + 312

324 = 312 * 1 + 12

312 = 12 * 16

Hence, gcd (9888, 6060) = 12.

38. gcd $(2^a-1, 2^b-1) = 2^{gcd(a,b)}-1$

-gcd$(2^{35}-1, 2^{34}-1) = 2^{gcd(35,34)} -1 = 2 - 1 = 1$

-gcd$(2^{35}-1, 2^{33}-1) = 2^{gcd(35,33)} -1 = 2 - 1 = 1$

-gcd$(2^{35}-1, 2^{31}-1) = 2^{gcd(35,31)} -1 = 2 - 1 = 1$

-gcd$(2^{35}-1, 2^{29}-1) = 2^{gcd(35,29)} -1 = 2 - 1 = 1$

-gcd$(2^{35}-1, 2^{23}-1) = 2^{gcd(35,23)} -1 = 2 - 1 = 1$

-gcd$(2^{34}-1, 2^{33}-1) = 2^{gcd(34,33)} -1 = 2 - 1 = 1$

gcd$(2^{34}-1, 2^{31}-1) = 2^{gcd(34,31)} -1 = 2 - 1 = 1$

$\gcd(2^{34}-1, 2^{29}-1) = 2^{\gcd(34,29)} - 1 = 2 - 1 = 1$

$\gcd(2^{34}-1, 2^{23}-1) = 2^{\gcd(34,23)} - 1 = 2 - 1 = 1$

$\gcd(2^{33}-1, 2^{31}-1) = 2^{\gcd(33,31)} - 1 = 2 - 1 = 1$

$\gcd(2^{33}-1, 2^{29}-1) = 2^{\gcd(33,29)} - 1 = 2 - 1 = 1$

$\gcd(2^{33}-1, 2^{23}-1) = 2^{\gcd(33,23)} - 1 = 2 - 1 = 1$

$\gcd(2^{31}-1, 2^{29}-1) = 2^{\gcd(31,29)} - 1 = 2 - 1 = 1$

$\gcd(2^{31}-1, 2^{23}-1) = 2^{\gcd(31,23)} - 1 = 2 - 1 = 1$

$\gcd(2^{29}-1, 2^{23}-1) = 2^{\gcd(29,23)} - 1 = 2 - 1 = 1$

Since all the *gcds* between each pair is 1, the integers $2^{35}-1$, $2^{34}-1$, $2^{33}-1$, $2^{31}-1$, $2^{29}-1$, and $2^{23}-1$ are pairwise relatively prime.

50. Since $a \equiv b$ (**mod** m), a **mod** $m = b$ **mod** m. Then suppose $a = t*m+r$ *and* $b = u*m+r$, that is, based on **LEMMA 1**, *gcd (a,m) = gcd (m,r)* and *gcd (b,m) = gcd (m,r).*
Thus *gcd (a,m) = gcd (b,m).*

54. Assume there are only finitely many primes,p_1, p_2, p_3...,p_n. Let $Q=3p_1p_2p_3...p_n-1$
($3k+2 = 3(k+1) -1$). There has no primes p_i that divides Q since suppose p_i is a factor of Q, p_i divides Q has a remainder p_i-1. But, based on the the fundamental theorem of arithmetic, Q can be written as a product of two or more primes. Since we have list all the primes while none of them can divides Q, then we can conclude that Q has at least one factor not in the list, p_1, p_2, p_3...,p_n, which is a contradiction with the assumption. Thus, there are infinitely many primes of form 3k+2.

4.4 Exercises ~~6, 8, 12, 16, 20, 23, 32, 33, 37~~

6. a) $17 = 8 * 2 + 1$
$2 = 1 * 2$
Inverse: $1 = 17 - 8 * 2$ Hence, -8 is an inverse of 2 modulo 17.

b) $89 = 34 * 2 + 21$
$34 = 21 * 1 + 13$
$21 = 13 * 1 + 8$
$13 = 8 * 1 + 5$
$8 = 5 * 1 + 3$
$5 = 3 * 1 + 2$
$3 = 2 * 1 + 1$
$2 = 1 * 2$
Inverse: $1 = 3 - 2 * 1$
$= 3 - (5 - 3 * 1) * 1 = -1 * 5 + 2 * 3$
$= -1 * 5 + 2 * (8 - 5 * 1) = 2 * 8 - 5 * 3$
$= 2 * 8 - 3 * (13 - 8 * 1) = -3 * 13 + 8 * 5$
$= -3 * 13 + 5 * (21 - 13 * 1) = 5 * 21 - 13 * 8$
$= 5 * 21 - 8 * (34 - 21 * 1) = -8 * 34 + 21 * 13$
$= -8 * 34 + 13 * (89 - 34 * 2) = 13 * 89 - 34 * 34$
Hence, -34 is an inverse of 34 modulo 89.

c) $233 = 144 * 1 + 89$
$144 = 89 * 1 + 55$
$89 = 55 * 1 + 34$

55 = 34 * 1 + 21

34 = 21 * 1 + 13

21 = 13 * 1 + 8

13 = 8 * 1 + 5

8 = 5 * 1 + 3

5 = 3 * 1 + 2

3 = 2 * 1 + 1

2 = 1 * 2

Inverse: 1 = 3 - 2 * 1

= 3 - 1 * (5 - 3 * 1) = -1 * 5 + 2 * 3

= -1 * 5 + 2 * (8 - 5 * 1) = 2 * 8 - 5 * 3

= 2 * 8 - 3 * (13 - 8 * 1) = -3 * 13 + 8 * 5

= -3 * 13 + 5 * (21 - 13 * 1) = 5 * 21 - 13 * 8

= 5 * 21 - 8 * (34 - 21 * 1) = -8 * 34 + 21 * 13

= -8 * 34 + 13 * (55 - 34 * 1) = 13 * 55 - 34 * 21

= 13 * 55 - 21 * (89 - 55 * 1) = -21 * 89 + 55 * 34

= -21 * 89 + 34 * (144 - 89 * 1) = 34 * 144 - 89 * 55

= 34 * 144 - 55 * (233 - 144 * 1) = -55 * 233 + 144 * 89

Hence, 89 is an inverse of 144 modulo 233.

d) 1001 = 200 * 5 + 1

200 = 1 * 200

Inverse: 1 = 1001 - 5 * 200

Hence, 5 is an inverse of 200 modulo 1001.

8. Suppose there exist an inverse of *a* modulo *m*, *i,* st. $a*i \equiv 1$ ***(mod** m)*. Let $a*i - 1 = m*q$ where *q* denotes the quotient. Suppose gcd (*a, m*) = *e*, which means *e* can divide *a* and *m*, then suppose $s*a + t*m = e$ (*s* and *t* are integers based on **Bezout's Theorem**), and *e* can divide results of any linear combinations of *a* and *m* since *s*a* and *t*m* always have a multiple relationship between *a* and *m*, that is, *e* is always a factor of *s*a* and *t*m*. Since $a*i - m*q$ is a form of linear combination of *a* and *m*, *e* can divide the result of such combination, which means *e* can divide 1. Thus the greatest value and the only possible value of *e* is 1 (*e* = 1, or gcd (*a,m*) = 1). We can prove that an inverse of *a* modulo *m* (>2) does not exist if gcd (*a,m*) >1 by applying contrapositive that if an inverse exists, then gcd (*a,m*) = 1.

12. a) 89 = 34 * 2 + 21

34 = 21 * 1 + 13

21 = 13 * 1 + 8

13 = 8 * 1 + 5

8 = 5 * 1 + 3

5 = 3 * 1 + 2

3 = 2 * 1 + 1

2 = 1 * 2

Inverse: 1 = 3 - 2 * 1

= 3 - 1 * (5 - 3 * 1) = -1 * 5 + 2 * 3

= -1 * 5 + 2 * (8 - 5 * 1) = 2 * 8 - 5 * 3

= 2 * 8 - 3 * (13 - 8 * 1) = -3 * 13 + 8 * 5

= -3 * 13 + 5 * (21 - 13 * 1) = 5 * 21 - 13 * 8

= 5 * 21 - 8 * (34 - 21 * 1) = -8 * 34 + 21 * 13

= -8 * 34 + 13 * (89 - 34 * 2) = 13 * 89 - 34 * 34

Hence, -34 is an inverse, -34 * 34 ≡ 1 (**mod** 89).

-34 * 34 x ≡ -34 * 77 (**mod** 89)

x ≡ -2618 (**mod** 89)

x ≡ 52 (**mod** 89)

The general solution is 89*k + 52. (k is an integer).

b) 233 = 144 * 1 + 89

144 = 89 * 1 + 55

89 = 55 * 1 + 34

55 = 34 * 1 + 21

34 = 21 * 1 + 13

21 = 13 * 1 + 8

13 = 8 * 1 + 5

8 = 5 * 1 + 3

5 = 3 * 1 + 2

3 = 2 * 1 + 1

2 = 1 * 2

Inverse: 1 = 3 - 2 * 1

= 3 - 1 * (5 - 3 * 1) = -1 * 5 + 2 * 3

= -1 * 5 + 2 * (8 - 5 * 1) = 2 * 8 - 5 * 3

= 2 * 8 - 3 * (13 - 8 * 1) = -3 * 13 + 8 * 5

= -3 * 13 + 5 * (21 - 13 * 1) = 5 * 21 - 13 * 8

= 5 * 21 - 8 * (34 - 21 * 1) = -8 * 34 + 21 * 13

= -8 * 34 + 13 * (55 - 34 * 1) = 13 * 55 - 34 * 21

= 13 * 55 - 21 * (89 - 55 * 1) = -21 * 89 + 55 * 34

= -21 * 89 + 34 * (144 - 89 * 1) = 34 * 144 - 89 * 55

= 34 * 144 - 55 * (233 - 144 * 1) = -55 * 233 + 144 * 89

Hence, 89 is an inverse, 144 * 89 ≡ 1 (mod 233).

144 * 89 x ≡ 89 * 4 (**mod** 233)

x ≡ 356 (**mod** 233)

x ≡ 123 (**mod** 233)

The general solution is 233 * k + 123 (k is an integer).

c) 1001 = 200 * 5 + 1

200 = 1 * 200

Inverse: 1 = 1001 - 200 * 5

Hence, -5 is an inverse, 200 * -5 ≡ 1 (mod 1001).

200 * -5 x ≡ -5 * 13 (**mod** 1001)

x ≡ -65 (**mod** 1001)

x ≡ 936 (**mod** 1001)

The general solution is 1001 * k + 936 (k is an integer).

16. a) 2*6≡1(**mod** 11)

3*4≡1(**mod** 11)

5*9≡1(**mod** 11)

7*8≡1(**mod** 11)

b) 10! = 1*2*3*4*5*6*7*8*9*10 = 10*(2*6)*(4*3)*(5*9)*(7*8)≡10(**mod** 11)≡-1(**mod** 11)

20. $M_1 = 60 / 3 = 20$, $M_2 = 60 / 4 = 15$, $M_3 = 60 / 5 = 12$.

$y_1 = 2$, $y_2 = 3$, $y_3 = 3$.

$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2*20*2+1*15*3+3*12*3 = 233 \equiv 53$ **mod** (60)

The general solution is 60 * k + 53 (k is an integer)

23. The first congruence $x \equiv 2$ (**mod** 3) can be expressed as $x = 3t + 2$ where t is an integer.

Then, $3t + 2 \equiv 1$ (**mod** 4)

$t \equiv 1$ (**mod** 4)

$t = 4u+1$

Take $t = 4u+1$ back into $x = 3t+2$, then we get $x = 12u + 5$.

Then, $12u + 5 \equiv 3$ (**mod** 5)

$u \equiv 4$ (**mod** 5)

$u = 5v+4$

Take $u = 5v + 4$ back into $x = 12u + 5$, then we get $x = 60v + 53$.

Thus, $x \equiv 53$ (**mod** 60).

32. Since the integers are divisible by 5 and has remainder 1 when divided by 3, suppose the integers as x, then $x \equiv 0$ (mod 5) and $x \equiv 1$ (mod 3).

Let $m_1 = 5$ and $m_2 = 3$; $a_1 = 0$ and $a_2 = 1$; then $M_1 = 15 / 5 = 3$ and $M_2 = 15 / 3 = 5$.

Then $y_1 = 2$ and $y_2 = 2$.

$x \equiv a_1M_1y_1 + a_2M_2y_2 = 0 * 3 * 2 + 1 * 5 * 2 = 10 \equiv 10$ (mod 15)

The general solution is 15 * k + 10 (k is an integer), for example, 10, 25,… and -5, -20….

33. Since $7^{12} \equiv 1$ (mod 13), $(7^{12})^k \equiv 1$ (mod 13) for every positive integer k.

$7^{121} = (7^{12})^{10}*7 \equiv 1^{10}*7 \equiv 7$ (mod 13)

Thus, $7^{121} \equiv 7$ (mod 13)

37. a) Since $2^{10} \equiv 1$ (mod 11), $(2^{10})^k \equiv 1$ (mod 11) for every positive integer k.

$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1$ (mod 11).

b) Since $32 \equiv 1$ (mod 31), $(32)^k \equiv 1$ (mod 31) for every positive integer k.

$2^{340} = (2^5)^{68} = 32^{68} \equiv 1^{68} \equiv 1$ (mod 31).

c) Since $2^{340} \equiv 1$ (mod 11) and $2^{340} \equiv 1$ (mod 31), 11 and 31 can divide $2^{340} – 1$, which means, $2^{340} – 1 \equiv 0$ (mod 11) and $2^{340} – 1 \equiv 0$ (mod 13). We can write $2^{340} – 1$ as a product of two of more primes, since 11 and 13 are prime and relatively prime, $2^{340} – 1 = 11*13*t = 341*t$, where t denotes the rest series of the primes. Thus, 341 can divide $2^{340} – 1$, and we can conclude that $2^{340} – 1 \equiv 0$ (mod 341).

4.5 Exercises ~~2, 5, 18, 32~~

2. a) h(104578690) = 104578690 mod 101 = 58

b) h(432222187) = 432222187 mod 101 = 60

c) h(372201919) = 372201919 mod 101 = 52

d) h(501338753) = 501338753 mod 101 = 3

5. $x_0 = 1$, $x_1 = (3x_0 + 2) \bmod 13 = 5 \bmod 13 = 5$

$x_1 = 5$, $x_2 = (3x_1 + 2) \bmod 13 = 17 \bmod 13 = 4$

$x_2 = 4$, $x_3 = (3x_2 + 2) \bmod 13 = 14 \bmod 13 = 1$

Because $x_3 = x_0$ and each term depends only on the previous term, the sequence 1, 5, 4, 1, 5, 4, 1, … is generated. This sequence contains 3 different numbers before repeating.

18. $x_{11} = x_1 + x_2 + x_3 + \ldots + x_n \bmod 9$

a) 7555618873

$x_{11} = 7 + 5 + 5 + 5 + 6 + 1 + 8 + 8 + 7 + 3 \bmod 9 = 55 \bmod 9 = 1$

b) 6966133421

$x_{11} = 6 + 9 + 6 + 6 + 1 + 3 + 3 + 4 + 2 + 1 \bmod 9 = 41 \bmod 9 = 5$

c) 8018927435

$x_{11} = 8 + 0 + 1 + 8 + 9 + 2 + 7 + 4 + 3 + 5 \bmod 9 = 47 \bmod 9 = 2$

d) 3289744134

$x_{11} = 3 + 2 + 8 + 9 + 7 + 4 + 4 + 1 + 3 + 4 \bmod 9 = 45 \bmod 9 = 0$

32. a) $d_8 \equiv 1*3+5*4+7*5+0*6+8*7+6*8+8*9 \pmod{11}$

$\equiv 234 \pmod{11}$

$\equiv 3 \pmod{11}$

The check digit is 3.

b) $d_8 \equiv 1*3+5*4+5*5+3*6+7*7+3*8+4*9 \pmod{11}$

$\equiv 175 \pmod{11}$

$\equiv 10 \pmod{11}$

The check digit is X.

c) $d_8 \equiv 1*3+0*4+8*5+9*6+7*7+0*8+8*9 \pmod{11}$

$\equiv 218 \pmod{11}$

$\equiv 9 \pmod{11}$

The check digit is 9.

d) $d_8 \equiv 1*3+3*4+8*5+3*6+8*7+1*8+1*9 \pmod{11}$

$\equiv 146 \pmod{11}$

$\equiv 3 \pmod{11}$

The check digit is 3.

4.6 Exercises ~~2, 5, 9, 10, 17, 24, 25~~

2. Replace STOP POLLUTION with numbers: 18-19-14-15 15-14-11-11-20-19-8-14-13

a) $f(p) = (p + 4) \bmod 26$

22-23-18-19 19-18-15-15-24-23-12-18-17

The encrypted message: WXST TSPPYXMSR

b) $f(p) = (p + 21) \bmod 26$

13-14-9-10 10-9-6-6-15-14-3-9-8

The encrypted message: NOJK KJGGPODJI

c) $f(p) = (17p + 22) \bmod 26$

16-7-0-17 17-0-1-1-24-7-2-0-9

The encrypted message: QHAR RABBYHCAJ

5. The decryption can be carried out using $f^{-1}(p) = (p - 10)$ **mod** 26.

a) CEBBOXNOB XYG

2-4-1-1-14-23-13-14-1 23-24-6

Replace each of the numbers by $f^{-1}(p) = (p - 10)$ **mod** 26:

18-20-17-17-4-13-3-4-17 13-14-22

The message is SURRENDER NOW.

b) LO WI PBSOXN

11-14 22-8 15-1-18-14-23-13

Replace each of the numbers by $f^{-1}(p) = (p - 10)$ **mod** 26:

1-4 12-24 5-17-8-4-13-3

The message is BE MY FRIEND.

c) DSWO PYB PEX

3-18-22-14 15-24-1 15-4-23

Replace each of the numbers by $f^{-1}(p) = (p - 10)$ **mod** 26:

19-8-12-4 5-14-17 5-20-13

The message is TIME FOR FUN.

9. The nine most common letters in English text and their approximate relative frequencies are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%. Suppose the shift cipher is $f(p) = (p + k)$ **mod** 26. The most frequent letter in the ciphertext is "M". Suppose "M" is corresponding to "E" because of the highest frequency, then k, the key, is 8 since "M" is 12 and "E" is 4, but it does not make sense for ERC = MZK; then suppose "M" is corresponding to "T", again it does not make sense for ERC. Repeat this procedure until the message makes sense, we can find that if "M" is corresponding to "I", ERC = ANY. Then we obtain the shift cipher, $f(p) = (p + 4)$ **mod** 26, since "M" is 12 and "I" is 8, and the inverse of it is $f^{-1}(p) = (p - 4)$ **mod** 26. Then we replace the letters in the ciphertext to numbers: 4-17-2 22-24-9-9-12-6-12-8-17-23-15-2 4-7-25-4-17-6-8-7 23-8-6-11-17-18-15-18-10-2 12-22 12-17-7-12-22-23-12-17-10-24-12-22 11-4-5-15-8 9-21-18-16 16-4-10-12-6. Replace each of the numbers by $f^{-1}(p) = (p - 4)$ **mod** 26: 0-13-24 18-20-5-5-8-2-8-4-13-19-11-24 0-3-21-0-13-2-4-3 19-4-2-7-13-14-11-14-6-24 8-18 8-13-3-8-18-19-8-13-6-20-8-18-7-0-1-11-4 5-17-14-12 12-0-6-8-2. The message is ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC.

10. Suppose the encryption function is $f(p) = (p + k)$ **mod** 26 and the decryption function is $f^{-1}(p) = (p - k)$ **mod** 26. Since the key in the encryption function is identical with that in the decryption function, k can be 0 or 13 that can convert letters to the same outputs. That is, for $k = 0$, $f(p) = (p)$ **mod** 26 and $f^{-1}(p) = (p)$ **mod** 26; and for $k = 13$, $f(p) = (p + 13)$ **mod** 26 and $f^{-1}(p - 13) = (p)$ **mod** 26.

17. The type of cipher may be an affine cipher since every letter in the cipertext has only one corresponding letter in the plaintext by their same frequency, and vice versa. This follows the rule of affine transformation which is a bijection.

24. ATTACK in numerical equivalents: 0019 1900 0210

gcd (13, (43-1)*(59-1)) = 1

$C = M^e \bmod n$

$= M^{13} \bmod (43*59)$

$0019^{13} \bmod 2537 \quad 1900^{13} \bmod 2537 \quad 0210^{13} \bmod 2537$

$= 2299 \qquad = 1317 \qquad = 2117$

Thus, the encrypted message is 2299 1317 2117.

25. UPLOAD in numerical equivalents: 2015 1114 0003

gcd (13, (53-1)*(61-1)) = 1

$C = M^e \bmod n$

$= M^{17} \bmod (53*61)$

$2015^{17} \bmod 3233 \quad 1114^{17} \bmod 3233 \quad 0003^{17} \bmod 3233$

$= 2545 \qquad = 2757 \qquad = 1211$

Thus, the encrypted message is 2545 2757 1211.