Assignment 3

Yang David Zhou, ID 260517397

October 23, 2014

Problem 1. *Prime Factorisation.*

Solution. (a) Prime Factorisation of 419
419 is a prime number

(b) Prime Factorisation of 9555
$9555 = 3 \cdot 5 \cdot 7^2 \cdot 13$

(c) Prime Factorisation of 10!
$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$
$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

Problem 2. *Euclid's Algorithm.*

Solution. (a) Find $d = \gcd(177, 38)$

$\gcd(177, 38) = \gcd(38, 25)$
$\gcd(38, 25) = \gcd(25, 13)$
$\gcd(13, 12) = \gcd(12, 1)$
$\gcd(12, 1) = \gcd(1, 0)$
$d = 1$

(b) Find $s, t \in \mathbb{Z}$ such that $d = 38s + 177t$

$d = 1$
$d = 13 - 12$
$d = 13 - (25 - 13) = 2 \cdot 13 - 25$
$d = 2 \cdot (38 - 25) - 25 = 2 \cdot 38 - 3 \cdot 25$
$d = 2 \cdot 38 - 3 \cdot (177 - 4 \cdot 38) = 14 \cdot 38 - 3 \cdot 177$
In $d = 38(14) + 177(-3)$, we have $s = 14, t = -3$

Problem 3. *Greatest Common Divisors.*

Solution. (a) Suppose that $\gcd(a, y) = 1$ and $\gcd(b, y) = d$. Prove that $\gcd(a \cdot b, y) = d$.

By Bezouts' Lemma we have the following:

(1) $\gcd(b, y) = d = sb + ty$
(2) $\gcd(a, y) = 1 = s'a + t'y$
Where $s, t, s', t' \in \mathbb{Z}$
So we can take (1) and multiply all the terms in it by 1,
$d(1) = sb(1) + ty(1)$
And substitute with (2),
$d = sb(s'a + t'y) + ty$
And rearrange,
$d = sbs'a + sbt'y + ty$
$d = ss'ab + (sbt' + t)y$

In the definition, s, s', t, t', b are all integers. Thus, we can show that d as the sum of ab and y each multiplied by an integer, i.e.,
$\gcd(ab, y) = i \cdot (a \cdot b) + j \cdot y$

Finally we know that d is identical in (1) and in $d = ss'ab + (sbt' + t)y$

(b) Suppose that $\gcd(b, a) = 1$. Prove that $\gcd(b + a, b - a) \leq 2$.

Problem 4. *Pseudorandom Numbers.*

Solution. (a) $x_{k+1} = 11x_k + 37 \mod 100$ with seed $x_0 = 52$
$x_0 = 52$
$x_1 = 11(52) + 37 \mod 100 = 9$
$x_2 = 11(9) + 37 \mod 100 = 36$
$x_3 = 11(36) + 37 \mod 100 = 33$
$x_4 = 11(33) + 37 \mod 100 = 0$
$x_5 = 11(0) + 37 \mod 100 = 37$
$x_6 = 11(37) + 37 \mod 100 = 44$
$x_7 = 11(44) + 37 \mod 100 = 21$
$x_8 = 11(21) + 37 \mod 100 = 68$
$x_9 = 11(68) + 37 \mod 100 = 85$
$x_{10} = 11(85) + 37 \mod 100 = 72$

(b) $x_{k+1} = 8x_k + 24 \mod 128$ with seed $x_0 = 0$
$x_0 = 0$
$x_1 = 8(0) + 24 \mod 128 = 24$
$x_2 = 8(24) + 24 \mod 128 = 88$
$x_3 = 8(88) + 24 \mod 128 = 88$
$x_4 = 8(88) + 24 \mod 128 = 88$
$x_5 = 8(88) + 24 \mod 128 = 88$
$x_6 = 8(88) + 24 \mod 128 = 88$
$x_7 = 8(88) + 24 \mod 128 = 88$
$x_8 = 8(88) + 24 \mod 128 = 88$
$x_9 = 8(88) + 24 \mod 128 = 88$
$x_{10} = 8(88) + 24 \mod 128 = 88$

Problem 5. *Modular Equations.*

Solution. Solve for x in $169x = 10 \mod 419$ with the modular inverse of 169.

$\gcd(419, 169)$
$= \gcd(169, 81)$
$= \gcd(81, 7)$
$= \gcd(7, 4)$
$= \gcd(4, 3)$
$= \gcd(3, 1)$
$= \gcd(1, 0) = 1$

$1 = 1(3) - 2(1)$
$1 = 1(3) - 2(4 - 3) = 3(3) - 2(4)$
$1 = 3(7 - 4) - 2(4) = 3(7) - 5(4)$
$1 = 3(7) - 5(81 - 11(17)) = 58(7) - 5(81)$
$1 = 58(169 - 2(81)) - 5(81) = 58(169) - 121(81)$
$1 = 58(169) - 121(419 - 2(169))$
$1 = 300(169) - 121(419)$
$169^{-1} = s = 300 \mod 419$

Now that we have obtained the modular inverse, we can solve the equation:
$169x = 10 \mod 419$
$169^{-1} \cdot 169x = 169^{-1} \cdot 10 \mod 419$
$x = 300 \cdot 10 \mod 419$
$x = 3000 \mod 419$
$x = 67$

Problem 6. *Congruences.*

Solution. (a) Evaluate $6022^{1267} \mod 17$
Here we apply Fermat's Little Theorem to evaluate,
$6022^{1267} \mod 17$
6022 can be rewritten as $6022 = 354 \cdot 17 + 4$, so by property of modulus,
$= 4^{1267} \mod 17$
$= 2^{2534} \mod 17$
$= 2^{158(16)+6} \mod 17$
$= (2^{16})^{158} \cdot 2^{6} \mod 17$
$= ((2^{16} \mod 17)^{158} \cdot 2^{6} \mod 17) \mod 17$
Since $2 \nmid 17$ as clearly $\gcd(17, 2) = 1$,
$= ((1)^{158} \cdot 64 \mod 17) \mod 17$
$= ((13) \mod 17$
$= 13$

(b) Evaluate $3^{42637} \mod 419$
Again, we apply FLT to evaluate,
$3^{42637} \mod 419$

$= 3^{102(418)+1} \mod 419$
$= (3^{418})^{102} \cdot 3^1 \mod 419$
$= ((3^{418} \mod 419)^{102} \cdot 3^1 \mod 419) \mod 419$
Since $3 \nmid 419$ as clearly $\gcd(419, 3) = 1$,
$= ((1)^{102} \cdot 3) \mod 419$
$= 3 \mod 419$
$= 3$