MATH 240 - Assignment 3

Jeremie Poisson - McGill ID 260627104

October 28th 2015

(I worked with Ellen Chen)

1 Prime factorisation

(a) *Prime factorisation of 511*

$$511 \div 7 = 73$$

Whereas 7 and 73 are primes. Therefore, the prime factorisation of 511 is:

$$511 = 7^1 * 73^1$$

(b) *Prime factorisation of 8085*

$$8085 \div 5 = 1617$$

$$1617 \div 3 = 539$$

$$539 \div 7 = 77$$

$$77 \div 7 = 11$$

The prime factorisation is then:

$$8085 = 11^1 * 7^2 * 5^1 * 3^1$$

(c) *Prime factorisation of 12!*

It is possible to develop the factorial notation and find prime factors of each factors.

$$12! = 12 * 11 * 10 * 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1$$

Now we simply have to find the prime factorisation of each factor.

$$12 = 3 * 4 = 3 * 2^2$$

$$\begin{aligned}
&11\\
10 &= 5 * 2\\
9 &= 3^2\\
8 &= 2^3\\
&7\\
6 &= 3 * 2\\
&5\\
4 &= 2^2\\
&3\\
&2\\
&1
\end{aligned}$$

Hence, the factorisation of 12! is :

$$12! = 11^1 * 7^1 * 5^2 * 3^5 * 2^{10}$$

2 Euclid's algorithm

(a) *Use Euclid's algorithm to* $d = gcd(561; 234)$

$$\begin{aligned}
gcd(561;234) &\qquad 561 = 234(2) + 93\\
gcd(93;234) &\qquad 234 = 93(2) + 48\\
gcd(93;48) &\qquad 93 = 48(1) + 45\\
gcd(45;48) &\qquad 48 = 45(1) + 3\\
gcd(45;3) &\qquad 45 = 3(15) + 0\\
&= 3
\end{aligned}$$

The greatest common divisor of 561 and 234 is 3.

(b) *Find integers* s *and* t *such that* $d = 234s + 561t$

We run the extended Euclid's algorithm.

$$\begin{aligned}
3 &= 48 + 45(-1)\\
&= 48 + (93 + 48(-1))(-1)\\
&= 48(2) + 93(-1)\\
&= (234 + 93(-2))(2) + 93(-1)\\
&= 234(2) + 93(-5)\\
&= 234(2) + (561 + 234(-2))(-5)\\
3 &= 234(12) + 561(-5)\\
&\Rightarrow s = 12 \qquad \Rightarrow t = -5
\end{aligned}$$

3 Greatest common divisors

(a) *Supposing that* $gcd(a, y) = d_1$ *and* $gcd(b, y) = d_2$*, prove that :*

$$gcd(gcd(a, b), y) = gcd(d_1, d_2)$$

Proof. Having the above relation, we can establish that :

$$d_1 \mid a \Rightarrow a = d_1 * s \qquad d_2 \mid b \Rightarrow b = d_2 * s'$$

$$d_1 \mid y \Rightarrow y = d_1 * t \qquad d_2 \mid y \Rightarrow y = d_2 * t'$$

where s, t, s', t' are some constants $\in \mathbb{R}$

Let $d_3 = gcd(a, b)$ for simplicity purposes. Therefore :

$$d_3 \mid a \Rightarrow a = d_3 * x$$

$$d_3 \mid b \Rightarrow b = d_3 * y$$

where x, y are some constants $\in \mathbb{R}$

$$a = d_1 * s \Rightarrow d_3 * x = d_1 * s \Rightarrow d_3 = d_1 * S$$
$$b = d_2 * s' \Rightarrow d_3 * y = d_2 * s' \Rightarrow d_3 = d_2 * S'$$

where S, S' are some constants $\in \mathbb{R}$

Hence,

$$d_1 \mid d_3 \quad \text{and} \quad d_2 \mid d_3$$

We already know that, if $d \mid a$ and $d \mid b$, then $d \mid gcd(a, b)$.

$$\text{if } (d_1 \mid d_3) \text{ and } (d_1 \mid y) \text{ then } \quad d_1 \mid gcd(d_3, y)$$
$$\text{if } (d_2 \mid d_3) \text{ and } (d_2 \mid y) \text{ then } \quad d_2 \mid gcd(d_3, y)$$

This also means that

$$gcd(d_3, y) > d_1 \quad \text{and} \quad gcd(d_3, y) > d_2$$

Hence :

$$gcd(d_3, y) = gcd(d_1, d_2) \Rightarrow$$
$$gcd(gcd(a, b), y) = gcd(d_1, d_2)$$

□

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

Proof. We already know that if $gcd(b, a)$ must divide $(b + a)$ and $(b - a)$. Therefore,

$$gcd(b + a, b - a) \mid (b + a) + (b - a) \Rightarrow gcd(b + a, b - a) \mid 2b$$
$$gcd(b + a, b - a) \mid (b + a) - (b - a) \Rightarrow gcd(b + a, b - a) \mid 2a$$

We also know that, if $x \mid a$ and $x \mid b$ then $x \mid gcd(a, b)$. Applying this to the result above we get :

$$gcd(b + a, b - a) \mid gcd(2b, 2a)$$

However, we already know that $gcd(b, a) = 1$, therefore $gcd(2b, 2a)$ is clearly 2 as there is no other common multiples between a and b (they are co-primes).

$$\Rightarrow gcd(b + a, b - a) \mid 2$$

It follows that

$$2 \leq gcd(b + a, b - a)$$

$\square$

4 Modular equations

Solve the modular equation

$$778x \equiv 20 \pmod{379}$$

Let's execute the extended Euclid's algorithm to find the greatest common divisor of $(778; 379)$.

$$\begin{aligned} gcd(778; 379) &\qquad 778 = 379(2) + 20 \\ gcd(20; 379) &\qquad 379 = 20(18) + 19 \\ gcd(20; 19) &\qquad 20 = 19(1) + 1 \\ gcd(1; 19) &\qquad 19 = 1(19) + 0 \\ &= 1 \end{aligned}$$

The numbers 778 and 379 are co-primes. We can find the inverse of 778 by running the extended Euclid's algorithm.

$$1 = 20 + 19(-1)$$
$$= 20 + (379 + 20(-18))(-1)$$
$$= 20(19) + 379(-1)$$
$$= (778 + 379(-2))(19) + 379(-1)$$
$$= 778(19) + 379(-39)$$

It follows that : $778^{-1} \pmod{379} \equiv 19$

$$778x \equiv 20 \pmod{379}$$
$$778 * 778^{-1}x \equiv 20 * 19 \pmod{379}$$
$$x \equiv 380 \pmod{379}$$
$$x \equiv 1 \pmod{379}$$

5 Pseudorandom numbers generation

Find the first 10 numbers given by the following linear congruence generators:

(a) $x_{k+1} = 13x_k + 41 \pmod{100}$, with seed $x_0 = 31$

$$x_1 = 13(31) + 41 = 444 = 44 \pmod{100}$$
$$x_2 = 13(44) + 41 = 613 = 13 \pmod{100}$$
$$x_3 = 13(13) + 41 = 210 = 10 \pmod{100}$$
$$x_4 = 13(10) + 41 = 171 = 71 \pmod{100}$$
$$x_5 = 13(71) + 41 = 964 = 64 \pmod{100}$$
$$x_6 = 13(64) + 41 = 873 = 73 \pmod{100}$$
$$x_7 = 13(73) + 41 = 990 = 90 \pmod{100}$$
$$x_8 = 13(90) + 41 = 1211 = 11 \pmod{100}$$
$$x_9 = 13(11) + 41 = 184 = 84 \pmod{100}$$
$$x_{10} = 13(84) + 41 = 1133 = 33 \pmod{100}$$

(b) $x_{k+1} = 13x_k + 41 \pmod{100}$, with seed $x_0 = 47$

$$x_1 = 13(47) + 41 = 652 = 52 \pmod{100}$$
$$x_2 = 13(52) + 41 = 717 = 17 \pmod{100}$$
$$x_3 = 13(17) + 41 = 262 = 62 \pmod{100}$$
$$x_4 = 13(62) + 41 = 847 = 47 \pmod{100}$$
$$x_5 = 13(47) + 41 = 652 = 52 \pmod{100}$$
$$x_6 = 13(52) + 41 = 717 = 17 \pmod{100}$$
$$x_7 = 13(17) + 41 = 262 = 62 \pmod{100}$$
$$x_8 = 13(62) + 41 = 847 = 47 \pmod{100}$$
$$x_9 = 13(47) + 41 = 652 = 52 \pmod{100}$$
$$x_{10} = 13(52) + 41 = 717 = 17 \pmod{100}$$

(c) $x_{k+1} = 8x_k + 24 \pmod{128}$, with seed $x_0 = 0$

$$x_1 = 8(0) + 24 = 24 = 24 \pmod{128}$$
$$x_2 = 8(24) + 24 = 216 = 88 \pmod{128}$$
$$x_3 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_4 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_5 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_6 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_7 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_8 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_9 = 8(88) + 24 = 728 = 88 \pmod{128}$$
$$x_{10} = 8(88) + 24 = 728 = 88 \pmod{128}$$

6 Congruences

(a) $4762^{5367} \pmod{13}$

Since 13 is a prime, we know, by Fermat's Little Theorem that :

$$4762^{12} \equiv 1 \pmod{13}$$

Resolution :

$$\equiv (4762^{12})^{447} \cdot 4762^3 \pmod{13}$$
$$\equiv 4762^3 \pmod{13} \equiv 4^3 \pmod{13}$$
$$\equiv 64 \pmod{13} \equiv 12 \pmod{13}$$

(b) $2^{39674} \pmod{523}$

Since 523 is a prime, we know, by Fermat's Little Theorem that :

$$2^{522} \equiv 1 \pmod{523}$$

Resolution :

$$\equiv (2^{522})^{76} \cdot 2^2 \pmod{523}$$
$$\equiv 2^2 \pmod{523} \equiv 4 \pmod{523}$$