MATA02 - Final Review Seminar

(2016 Q2) Consider the numbers $m = 2^8 \cdot 3^5 \cdot 7^3 \cdot 17^4$ and $n = 2^5 \cdot 5^4 \cdot 7^2 \cdot 11^3$.

(a) How many positive whole numbers divide m?

$m = 2^8 \cdot 3^5 \cdot 7^3 \cdot 17^4$

$\Rightarrow (8+1)(5+1)(3+1)(4+1) = 9 \cdot 6 \cdot 4 \cdot 5 = 1080$ positive whole numbers divide m.

(b) How many positive integers divide both m and n?

$m = 2^8 \cdot 3^5 \cdot 7^3 \cdot 17^4$

$n = 2^5 \cdot 5^4 \cdot 7^2 \cdot 11^3$

$\Big\}$ $\gcd(m,n) = 2^5 \cdot 7^2$

$\Rightarrow (5+1)(2+1) = 6 \cdot 3 = 18$ positive integers divide both m and n.

(c) Compute $\phi(n)$

Euler's Phi

$$\phi(n) = \phi(p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}) = n\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_2-1}{p_2}\right)\cdots\left(\frac{p_k-1}{p_k}\right) \qquad \phi(p) = p-1$$

non-prime — prime

$n = 2^5 \cdot 5^4 \cdot 7^2 \cdot 11^3$

$$\phi(n) = \phi(2^5 \cdot 5^4 \cdot 7^2 \cdot 11^3) = 2^5 \cdot 5^4 \cdot 7^2 \cdot 11^3 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} \cdot \frac{10}{11}$$
$$= 2^4 \cdot 5^3 \cdot 7 \cdot 11^2 \cdot 2^2 \cdot 2 \cdot 3 \cdot 2 \cdot 5$$
$$= 2^8 \cdot 3 \cdot 5^4 \cdot 7 \cdot 11^2$$

(2016 Q3) Evaluate the fraction $\frac{2}{5}$ in arithmetic modulo 37.

Way ① $\frac{2}{5} \bmod 37 = x$

$\Rightarrow 2 \bmod 37 = 5x$

$\Rightarrow (-35) \bmod 37 = 5x$

$\Rightarrow \left(\frac{-35}{5}\right) \bmod 37 = x$

$\Rightarrow (-7) \bmod 37 = x$

$\Rightarrow 30 \bmod 37 = x$

$\therefore \frac{2}{5} \equiv 30 \bmod 37$

Way ② $\frac{2}{5} \bmod 37 = x$

$\Rightarrow 2 \bmod 37 = 5x$

$\gcd(37,5)$: $37 = 5 \times 7 + 2$

$5 = 2 \times 2 + 1$

$1 = 5 - 2 \times 2$

$1 = 5 - (37 - 5 \times 7) \times 2$

$(1 = 5 \times 15 - 37 \times 2) \times 2$

$2 = 5 \times 30 - 37 \times 4$

$37 \times 4 + 2 = 5 \times 30$

$2 \bmod 37 = 5 \times 30 \Rightarrow x = 30 \quad \therefore \frac{2}{5} \equiv 30 \bmod 37$

2 ways! You pick your favourite ☺

(2016 Q 4) Use Fermat's theorem to evaluate the power $2^{83} \bmod 23$

Fermat's Theorem
If p is prime and a is non zero on modulo p, then $a^{p-1} \equiv 1 \bmod p$.

By Fermat's Thm $2^{22} \equiv 1 \bmod 23$

$83 = 22 \times 3 + 17 \rightarrow 2^{83} \equiv 2^{22\times3+17} \equiv (2^{22})^3 (2^{17}) \equiv 2^{17} \bmod 23$

$2^2 \equiv 4 \bmod 23$
$2^4 \equiv 4^2 \equiv 16 \equiv (-7) \bmod 23$
$2^8 \equiv (-7)^2 \equiv 49 \equiv 3 \bmod 23$
$2^{16} \equiv (3)^2 \equiv 9 \bmod 23$
$2^{17} \equiv 2 \cdot 2^{16} \equiv 2 \cdot 9 \equiv 18 \bmod 23$

$\therefore 2^{83} \equiv 18 \bmod 23$.

(2016 Q5) Find the twenty-ninth root of 7, $\sqrt[29]{7}$, in arithmetic modulo 65.

Check for $\sqrt[k]{a} \bmod n$, in order to use this method
- a and n are relatively prime
- k and $\phi(n)$ are relatively prime

Check: $k=29$, $a=7$, $n=65$

- 7 and 65 are relatively prime
- 29 and 48 are relatively prime

Side:
$65 = 5 \times 13$

$\phi(65) = 5 \times 13 \times \frac{4}{5} \times \frac{12}{13} = 48 = 2^4 \cdot 3$

We can find a solution for $1 = 29m - 48\ell$

$\gcd(29, 48)$

$48 = 29 \times 1 + 19$
$29 = 19 \times 1 + 10$
$19 = 10 \times 1 + 9$
$10 = 9 \times 1 + 1$

$1 = 10 - 9 \times 1$
$1 = 10 - (19 - 10 \times 1) \times 1$
$1 = 10 \times 2 - 19 \times 1$
$1 = (29 - 19 \times 1) \times 2 - 19 \times 1$
$1 = 29 \times 2 - 19 \times 3$
$1 = 29 \times 2 - (48 - 29 \times 1) \times 3$
$1 = 29 \times 5 - 48 \times 3$ (*)

($5 = m$)

Verify $7^5 \equiv \sqrt[29]{7} \bmod 65$

$(7^5)^{29} \equiv (\sqrt[29]{7})^{29} \bmod 65$
$7^{5\times29} \equiv 7 \bmod 65$

Euler's
If k is $\phi(n)$ and a is non zero on modulo p, then $a^k \equiv 1 \bmod n$

(*) $5 \times 29 = 1 + 48 \times 3$ — By Euler's $7^{48} \equiv 1 \bmod 65$

$\Rightarrow 7^{5\times 29} \equiv 7^{1+48\times 3} \equiv 7 \cdot (7^{48})^3 \equiv 7 \bmod 65$ $\quad \therefore 7^5 \equiv \sqrt[29]{7} \bmod 65$

Now, let's find $7^5 \bmod 65$

$7^2 \equiv 49 \equiv (-16) \bmod 65$
$7^4 \equiv (-16)^2 \equiv 256 \equiv 61 \equiv (-4) \bmod 65$
$7^5 \equiv 7^4 \cdot 7 \equiv (-4)7 \equiv -28 \equiv 37 \bmod 65$

$\therefore \sqrt[29]{7} \equiv 37 \bmod 65$

(2016 Q7) You are an FBI agent who has just intercepted a message from mobster Tony Soprano to his enforcer, Peter Paulie Walnuts Gualtieri. Tony and Paulie are using the public-key modular arithmetic encryption system with modulus $n=77$ and exponent $k=11$, so that to encode his message Tony raises it to the 11^{th} power mod 77. The enciphered message that you intercept is 3. Find the original message

$n=77$ $\quad$ Message 3 $\quad$ A_1
$k=11$

Check: k and $\phi(n)$ relatively prime?
$\phi(77) = 7 \times 11 \times \frac{6}{7} \times \frac{10}{11} = 60 = 2^2 \cdot 3 \cdot 5$
$\therefore \gcd(11, 60) = 1$ ✓

$1 = 11m - 60l$

$\gcd(11,60) \rightarrow 60 = 11 \times 5 + 5$
$11 = 5 \times 2 + 1$

$1 = 11 - 5 \times 2$
$1 = 11 - (60 - 11 \times 5) \times 2$
$1 = 11 - 60 \times 2 + 11 \times 10$
$1 = 11 \times \underset{m}{11} - 60 \times 2$

$A_1^k \equiv 3^{11} \equiv 3^8 \cdot 3^2 \cdot 3 \equiv 16 \cdot 9 \cdot 3 \equiv 432 \equiv 47 \bmod 77$ $\quad \therefore B_1 = 47$ (encrypted)

$3^2 \equiv 9 \bmod 77$
$3^4 \equiv 81 \equiv 4 \bmod 77$
$3^8 \equiv 16 \bmod 77$

Decipher:

$B_1^m \equiv 47^{11} \equiv 47^8 \cdot 47^2 \cdot 47 \equiv (-17)(-24)47 \equiv 19176 \equiv 3 \bmod 77$ $\quad \therefore A_1 = 3$ (as wanted)

$47^2 \equiv 2209 \equiv 53 \equiv (-24) \bmod 77$
$47^4 \equiv (-24)^2 \equiv 576 \equiv 37 \bmod 77$
$47^8 \equiv (37)^2 \equiv 1369 \equiv 60 \equiv (-17) \bmod 77$

$\therefore$ Message $3 \rightarrow C$.

(2016 Q6) Use the divisibility tests to determine (a) if $n = 156783492$ is divisible by 3, 9 or 11 and (b) if $m = 4815713$ is divisible by 7.

Divisibility Tests

- Divisibility by 7 : A-2B
- Divisibility by 11 : alternating sum
- Divisibility by 13: A+4B or A-9B
- Divisibility by 17: A-5B
- Divisibility by 19: A+2B

(a) $n = 156783492$

Div 3: $1+5+6+7+8+3+4+9+2 = 45$

45 is div by 3, so n is div by 3 too.

Div 9: $1+5+6+7+8+3+4+9+2 = 45$

45 is div by 9, so n is div by 9 too.

Div 11: $2-9+4-3+8-7+6-5+1 = -3$

-3 is nod div by 11, so n is not div by 11.

(b) $m = 4815713$ (A = 481571, B = 3)

Div 7: $\rightarrow 481571 - 2\cdot 3 = 481565$

$\rightarrow 48156 - 2\cdot 5 = 48146$

$\rightarrow 4814 - 2\cdot 6 = 4802$

$\rightarrow 480 - 2\cdot 2 = 476$

$\rightarrow 47 - 2\cdot 6 = 35$

35 is div by 7, then m is div by 7 too.

(2017 Q 1) List all the prime numbers between 120 and 170. Show your work.

Eratosthene's Sieve

Find prime numbers in a given interval by iterating through the list of smaller prime numbers and checking divisibility

Find the root upper bound $\sqrt{170} < 14$

The set of primes less than 14 $\Rightarrow \{2, 3, 5, 7, 11, 13\}$

let's start crossing out the numbers that are divisible by 2 first, and then follow in order the set we defined above.

Step ① Cancel out #s divisible by 2
Step ② Cancel out #s divisible by 3
Step ③ Cancel out #s divisible by 5
Step ④ Cancel out #s divisible by 7
Step ⑤ Cancel out #s divisible by 11
Step ⑥ Cancel out #s divisible by 13

~~120~~ 121 ~~122~~ ~~123~~ ~~124~~ ~~125~~ ~~126~~ 127 ~~128~~ ~~129~~

~~130~~ 131 ~~132~~ ~~135~~ ~~134~~ ~~135~~ ~~136~~ 137 ~~138~~ 139

~~140~~ ~~141~~ ~~142~~ ~~143~~ ~~144~~ ~~145~~ ~~146~~ ~~147~~ ~~148~~ 149

~~150~~ 151 ~~152~~ ~~153~~ ~~154~~ ~~155~~ ~~156~~ 157 ~~158~~ ~~159~~

~~160~~ ~~161~~ ~~162~~ 163 ~~164~~ ~~165~~ ~~166~~ 167 ~~168~~ ~~169~~

~~170~~

∴ The prime numbers between 120 and 170 are:
127, 131, 137, 139, 149, 151, 157, 163, 167

(2017 Q5) Find the following 31st roots in arithmetic modulo 7.

(a) $\sqrt[31]{279} \bmod 7$

> Check for $\sqrt[k]{a} \bmod n$, in order to use this method
> - n is prime
> - k and n-1 are relatively prime
> - a non-zero in modulo n

Check:
- 7 is prime
- 31 and 7-1=6 are relatively prime
- 279 is non-zero in mod 7

We can find a solution for $1 = 31m - 6l$

$\gcd(31, 6)$ $\quad 31 = 6 \times 5 + 1$

$1 = 31 \times 1 - 6 \times 5$ (*)

Verify $279 \equiv \sqrt[31]{279} \bmod 7$

$(279)^{31} \equiv (\sqrt[31]{279})^{31} \bmod 7$

$279^{31} \equiv 279 \bmod 7$

(*) $31 = 1 + 6 \times 5$

By Fermat's: $279^6 \equiv 1 \bmod 7$

$\Rightarrow 279^{31} \equiv 279^{1+6\times5} \equiv 279 \cdot (279^6)^5 \equiv 279 \bmod 7$

$279 \equiv 6 \bmod 7$ $\quad\therefore \sqrt[31]{279} \equiv 6 \bmod 7$

(b) $\sqrt[31]{280} \bmod 7$

Let $\sqrt[31]{280} \bmod 7 = x$

$280 \bmod 7 = x^{31}$

$0 = x^{31}$

$x = 0$ $\quad\therefore \sqrt[31]{280} \equiv 0 \bmod 7$

(c) $\sqrt[31]{282} \bmod 7$

Check:
- 7 is prime
- 31 and $7-1=6$ are relatively prime
- 282 is non-zero in mod 7

} same as part (a)!

We can find a solution for $1 = 31m - 6l$

$\gcd(31, 6)$ $\quad 31 = 6\times5 + 1$

$1 = 31\times1 - 6\times5$ (*)

} same as part (a)!

verify $282 \equiv \sqrt[31]{282} \bmod 7$

$(282)^{31} \equiv (\sqrt[31]{282})^{31} \bmod 7$

$282^{31} \equiv 282 \bmod 7$

(*) $31 = 1 + 6 \times 5$

By Fermat's: $282^6 \equiv 1 \bmod 7$

$\Rightarrow 282^{31} \equiv 282^{1+6\times5} \equiv 282 \cdot (282^6)^5 \equiv 282 \bmod 7$

$282 \equiv 2 \bmod 7$

$\therefore \sqrt[31]{282} \equiv 2 \bmod 7$

(2017 Q6) Find 6 consecutive composite integers, that is 6 consecutive integers of which none is a prime number

$7!+2$, $7!+3$, $7!+4$, $7!+5$, $7!+6$, $7!+7$

Bonus: Can you find 6 such numbers that are smaller than 100?

91, 92, 93, 94, 95, 96