MATH135 Notes / Reminders (Assignment Review)

A9. Polar multiplication only works for MULTIPLICATON, NOT division

↳ e.g. $5(\cos 8\theta + i\sin 8\theta) \cdot 2(\cos\theta + i\sin\theta)$

$= 5 \cdot 2(\cos(8\theta+\theta) + i\sin(8\theta+\theta))$

$= 10(\cos 9\theta + i\sin 9\theta)$

MULTPLY	DIVIDE
mod × mod	mod ÷ mod
arg + arg	arg − arg

essentially DMT, not polar multiplication

A9 → Q1 → (a)(ii),

multiply top & bottom by conjugate, otherwise you are invoking DMT...

A8. RSA encryption: Public key: $(e, \underbrace{pq}_{\boxed{pq=n}})$

Private key: $(\underbrace{d}, pq)$

$\boxed{ed \equiv 1 \pmod{(p-1)(q-1)}}$

$1 < d < (p-1)(q-1)$

Square & multiply algorithm / modular exponentiation

$C \equiv M^e \pmod{n}$, $0 \leqslant C < n$

$\Rightarrow C \equiv 10^{23} \pmod{377}$, $0 \leqslant C < 377$

Using the "square and multiply" algorithm / modular exponentiation

$10^2 \equiv 100 \pmod{377} \longrightarrow 377 \mid 10^2 - 100 \Rightarrow 377 \mid 0$ (as $100 < 377$)

$10^4 \equiv (10^2)^2 \equiv \underline{198} \pmod{377}$ $\quad 10000 - 26(377) = \underline{198}$

squared squared

$10^8 \equiv (10^4)^2 \equiv 198^2 \equiv 373 \pmod{377}$

simplify further

$10^{16} \equiv (10^8)^2 \equiv 373^2 \equiv 139129 \equiv 16 \pmod{377}$

Also, $10^3 \equiv 1000 \equiv \underline{246} \pmod{377}$ $\quad 1000 - 2(377) = \underline{246}$

$10^{23} = 10^{16} \times 10^4 \times 10^3$, so $C \equiv 10^{16} \times 10^4 \times 10^3 \pmod{377}$

they are congruent to each other

$\equiv 16 \times 198 \times 246 \pmod{377}$

$\equiv 779328 \pmod{377} \equiv 69 \pmod{377}$

$C \equiv 69 \pmod{377}$

$377 \mid C - 69$

$377k = C - 69$, $k \in \mathbb{Z}$

let $k = 0$,

$C = 377(0) + 69 = 69$

Since $0 \leqslant 69 < 377$, $C = 69$ $\quad 779328 - 2067(377) = 69$

We must solve $C \equiv 10^{23} \pmod{377}$ for $0 \le C < 377$. Observe that

$$\begin{aligned}
10^2 &\equiv 100 \pmod{377} \\
10^4 &\equiv (10^2)^2 \equiv 100^2 \equiv 10000 \equiv 198 \pmod{377} \\
10^8 &\equiv (10^4)^2 \equiv 198^2 \equiv 39204 \equiv 373 \pmod{377} \\
10^{16} &\equiv (10^8)^2 \equiv 373^2 \equiv 139129 \equiv 16 \pmod{377}
\end{aligned}$$

Now,

$$\begin{aligned}
10^{23} &\equiv 10^{16} \cdot 10^4 \cdot 10^2 \cdot 10 \pmod{377} \\
&\equiv 16 \cdot 198 \cdot 100 \cdot 10 \pmod{377} \\
&\equiv 3168 \cdot 1000 \pmod{377} \\
&\equiv 152 \cdot 246 \pmod{377} \\
&\equiv 37392 \pmod{377} \\
&\equiv 69 \pmod{377}
\end{aligned}$$

Since $0 \le 69 < 377$, we know that the ciphertext is $C = 69$.

* Reminder about modular arithmetic:

$14 \pmod 5$

$14 \div 5 = 2$ remainder 4

$\therefore 14 \pmod 5 = \underline{4}$ ← the remainder

Since $7^2 \equiv 1 \pmod{12}$, $11 \equiv -1 \pmod{12}$, and $-23 \equiv 1 \pmod{12}$ using CP and CAM,

$$\begin{aligned}
&7^{135} + 4 \cdot 11^{2022} - 23 \pmod{12} \\
&\equiv 7(7^2)^{67} + 4 \cdot (11)^{2022} - 23 \pmod{12} \\
&\equiv 7(1)^{67} + 4(-11)^{2022} + 1 \pmod{12} \\
&\equiv 7 + 4 + 1 \pmod{12} \\
&\equiv 12 \pmod{12} \equiv 0 \pmod{12}
\end{aligned}$$

Since the remainder is zero, $7^{125} + 4 \cdot 11^{2022} - 23$ is divisible by 12

For all complex numbers z, the multiplicative inverse of z exists if and only if $z \neq 0$. Moreover, for $z = a + bi \neq 0$, the multiplicative inverse is unique, and is given by

$$\boxed{z^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = \frac{a-bi}{a^2+b^2}.}$$

multiplicative inverse

Find $[15]^{-1}$ in $\mathbb{Z}_{38}$

$\gcd(15, 38) = 1$, so $[15]^{-1}$ exists

Let $x = [15]^{-1}$, so $[15][15]^{-1} = [15]x = 1$

$[15]x = 1$

$15x \equiv 1 \pmod{38}$

$\downarrow$

$38 \mid 15x - 1 \Rightarrow 38y = 15x - 1$

$\Rightarrow 15x - 38y = 1$

Applying EEA, $x = -5$, $y = -2$

By LCT1, $x = -5 + 38n$, $(n \to -n)$

$\Rightarrow x \equiv -5 \pmod{38}$

So $x = [-5] = [-5 + 38] = [33]$

$\therefore [15]^{-1} = [33]$

* $[a]$ has multiplicative inverses in $\mathbb{Z}_m \Leftrightarrow \gcd(a, m) = 1$