Computational Number Thoery - Midterm Exam

Philip Warton

February 5, 2021

Problem 1

$$
\begin{aligned}
101 &= 8 \cdot 12 + 5 \\
77 &= 11 \cdot 7 + 0 \\
-40 &= -4 \cdot 11 + 4
\end{aligned}
$$

Problem 2

Use the extended Euclidean algorithm to show that $\gcd(14, 89) = 1$ and to find the smallest positive integer x satisfying $14x \equiv 1 \pmod{89}$.

$$
\begin{aligned}
89 &= (6)14 + 5 \\
14 &= (2)5 + 4 \\
5 &= (1)4 + 1 \\
4 &= (4)1 + 0
\end{aligned}
$$

$$
\begin{aligned}
5 - 4 &= 1 \\
5 - (14 - (2)5) &= 1 \\
(3)5 - 14 &= 1 \\
(3)(89 - (6)14) - 14 &= 1 \\
(3)89 - (19)14 &= 1
\end{aligned}
$$

Then we say that $14(-19) \equiv 1 \pmod{89}$ or equivalently $14(70) \equiv 1 \pmod{89}$.

Problem 3

Find the orders of 2 and 3 mod 13 Are either primitive roots? Recall first that if $a \equiv b \pmod{13}$ then of course $(c)a \equiv (c)b \pmod{13}$.

$$
\begin{aligned}
2^1 &\equiv 2 \\
2^2 &\equiv 4 \\
2^3 &\equiv 8 \\
2^4 &\equiv 16 \equiv 3 \\
2^5 &\equiv 6 \\
2^6 &\equiv 12 \\
2^7 &\equiv 24 \equiv 11 \\
2^8 &\equiv 22 \equiv 9 \\
2^9 &\equiv 18 \equiv 5 \\
2^{10} &\equiv 10 \\
2^{11} &\equiv 20 \equiv 7 \\
2^{12} &\equiv 14 \equiv 1
\end{aligned}
$$

We can compute these powers for the number 3 as well:

$$\begin{aligned}3^1 &\equiv 3\\ 3^2 &\equiv 9\\ 3^3 &\equiv 1\end{aligned}$$

Then since 2 has an order of 12, it is a primitive root mod 13. The number 3 has an order of 3 and is not a primitive root mod 13.

Problem 4

(a)

Proof. By assumption, we say that a is order 3 mod p. This means, $a^3 \equiv 1 \mod p$. Then, since p is prime and $a \nmid p$, by Fermat's Little Theorem we have $a^{p-1} \equiv 1 \mod p$. We know that the following pattern will be generated by multiplying a mod p:

$$\begin{aligned}a &\equiv x \mod p\\ a^2 &\equiv y \mod p\\ a^3 &\equiv 1 \mod p\\ a^4 &\equiv x \mod p\\ a^5 &\equiv y \mod p\\ a^6 &\equiv 1 \mod p\\ a^7 &\equiv x \mod p\\ &\vdots\\ a^{p-1} &\equiv 1 \mod p\end{aligned}$$

Since $\langle a \rangle \cong U_3$ and cycles every 3 powers, it follows that $p-1$ must be of the form $3k$ for some $k \in \mathbb{Z}$. So of course $p - 1 = 3k \implies p = 3k+1$ therefore $p \equiv 1 \mod 3$. $\square$

(b)

Proof. We want to show that $a^2 + a + 1 \equiv 0 \mod p$.

$$\begin{aligned}&(a-1)(a^2+a+1) = a^3 - 1\\ &a^3 \equiv 1 \mod p\\ &a^3 - 1 \equiv 0 \mod p\\ \implies &(a-1)(a^2+a+1) \equiv 0 \mod p\end{aligned}$$

Then it must be the case that either $a^2 + a + 1 \equiv 0 \mod p$ or that $a - 1 \equiv 0 \mod p$. If $a - 1 \equiv 0 \mod p$ then $a \equiv 1 \mod p$ and a would be order 1 mod p (contradiction, a is order 3 mod p). So it must be the case that $a^2 + a + 1 \equiv 0 \mod p$. $\square$

(c)

Proof. We want to show that $a + 1$ is order 6 mod p. Let us check each power $1, 2, \cdots, 5, 6$. Suppose that $a + 1 \equiv 1 \mod p$ then we would have $a \equiv 0 \mod p$, which by the order of a being 3 mod p we know to be false. So we check $(a+1)^2$, and in this case we say

$$(a+1)^2 = a^2 + 2a + 1 = a + (a^2 + a + 1) \equiv a + 0 \not\equiv 0 \mod p$$

Now we can check $(a+1)^3$, which can be rewritten as $(a+1)(a+1)^2$. Then

$$(a+1)^3 = (a+1)(a+1)^2 \equiv (a+1)a = a^2 + a \equiv -1 \mod p$$

We know this last equivalence by $\boxed{\text{b}}$. Then since a has order 3, we know that $p \neq 2$ and thus $1 \not\equiv -1 \mod p$. Since $(a+1)^2 \equiv a \mod p$, and since a is order 3, we can write

$$(a+1)^4 = ((a+1)^2)^2 \equiv (a)^2 \not\equiv 1 \mod p$$

Then for $(a+1)^5$, we write this as the following

$$(a+1)^5 = (a+1)^4(a+1) \equiv a^2(a+1) = a^3+1 \equiv 1+1 \not\equiv 1 \mod p$$

We know that $2 \neq 1 \mod p$ since $p \geqslant 3$. Finally we write

$$(a+1)^6 = (a+1)^3(a+1)^3 \equiv (-1)^2 \equiv 1 \mod p$$

So since the smallest power at which $(a+1)$ becomes equivalent to 1 is 6, we say that $a+1$ is order 6 mod p. $\square$