MATH 542 NUMBER THEORY
Problems to Think About #4
CH. 4, #1-4

Russell Jahn

February 24th, 2014

(1)

p prime, $p \equiv 1 (\text{mod } 4) \Rightarrow p = 1 + 4k$ some $k \in \mathbb{Z}$

g primitive (mod p) $\Rightarrow (g, p) = 1$ and $g^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$ (as in PTTA3 no.1)

Let $d = o(-g) \pmod{p}$

$(g, p) = 1 \Rightarrow (-g, p) = 1 \Rightarrow (-g)^{p-1} \equiv 1 (\text{mod } p) \quad \therefore d \mid p - 1$

$(-g)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} g^{\frac{p-1}{2}} \equiv (1)(-1) \equiv -1 (\text{mod } p)$

$\therefore d \nmid \frac{p-1}{2}$

So, $p - 1 = dl$ for some $l \in \mathbb{Z}$

$\Rightarrow \frac{p-1}{2} = \frac{dl}{2} \Rightarrow 2 \nmid l$ (since this $\Rightarrow d \mid \frac{p-1}{2}$)

$\Rightarrow 2 \mid d \Rightarrow d$ is even

$\Rightarrow 1 \equiv (-g)^d \equiv (-1)^d g^d \equiv g^d \pmod{p}$

$\Rightarrow d = p - 1$ (g primitive)

$\Rightarrow -g$ primitive (mod p) ✓

(2)

Let p, $2p + 1$ prime $\quad p \equiv 3 \pmod{4} \equiv -1 \pmod{4}$ $\quad$ Let $p = -1 + 4k$ for some $k \in \mathbb{Z}$

Clearly, $(-2, 2p + 1) = 1 \quad \therefore$ By Euler, $(-2)^{\phi(2p+1)} = (-2)^{2p} \equiv 1 \pmod{2p + 1}$

Let $d = o(-2) \pmod{2p + 1}$

$\therefore d \mid 2p \Rightarrow d \in \{1, 2, p, 2p\}$

Suppose $d = 1 \Rightarrow -2 \equiv 1 \pmod{2p + 1} \Rightarrow 3 \equiv 0 \pmod{2p + 1} \Rightarrow 2p + 1 \mid 3$

($\Rightarrow\Leftarrow$) since $2p + 1 \geq 7$

$\therefore d \neq 1$

Suppose $d = 2 \Rightarrow (-2)^2 \equiv 1 \pmod{2p + 1} \Rightarrow 4 \equiv 1 \pmod{2p + 1} \Rightarrow 3 \equiv 0 \pmod{2p + 1}$

Same as above $\quad \therefore d \neq 2$

Suppose $d = p \Rightarrow (-2)^p \equiv 1 \pmod{2p+1} \Rightarrow (-1)^p 2^p \equiv 1 \Rightarrow 2^p \equiv -1 \Rightarrow 2^{-1+4k} \equiv -1 \pmod{2p+1}$

$\Rightarrow 2^{4k} \equiv -2 \Rightarrow (2^{2k})^2 \equiv -2 \pmod{2p+1}$

$\therefore -2$ is a quadratic residue $\pmod{2p+1}$

$\therefore 1 = \left(\frac{-2}{2p+1}\right) = \left(\frac{-1}{2p+1}\right)\left(\frac{2}{2p+1}\right) = (-1)^{\frac{1}{2}(2p+1-1)}(-1)^{\frac{1}{8}(4p^2+4p+1-1)}$

$= (-1)^p(-1)^{\frac{1}{2}(p^2+p)} = (-1)^{-1+4k+\frac{1}{2}(1-8k+16k^2-1+4k)} = (-1)^{-1} = -1 \quad (\Rightarrow\Leftarrow)$

$\therefore d \neq p$

$\therefore d = 2p = \phi(2p+1) \Rightarrow -2$ is primitive $\pmod{2p+1}$ ✓

(3)

Note: $p,\ \ 2^k p + 1$ odd primes $\Rightarrow k \geq 1$

$(\Leftarrow)$ Let $d = o(a) \qquad \pmod{2^k p + 1}$

$a^{2^k} \not\equiv 1 \pmod{2^k p+1} \Rightarrow d \nmid 2^k$

$\left(\frac{a}{2^k p+1}\right) = -1 \Rightarrow (a, 2^k p + 1) = 1 \Rightarrow a^{(2^k p+1)-1} \equiv 1 \pmod{2^k p+1} \Rightarrow a^{2^k p} \equiv 1 \pmod{2^k p+1}$

$\therefore d \mid 2^k p$ and $d \nmid 2^k \Rightarrow d = 2^l p$ for some $l \leq k$

Now, $-1 = \left(\frac{a}{2^k p+1}\right) \equiv a^{\frac{1}{2}((2^k p+1)-1)} \pmod{2^k p+1} \equiv a^{2^{k-1}p} \pmod{2^k p+1}$

$\Rightarrow d \nmid 2^{k-1}p \Rightarrow k-1 < l \leq k \Rightarrow d = 2^k p = (2^k p + 1) - 1$

$\therefore a$ is primitive $\quad \pmod{2^k p+1}$

$(\Rightarrow)$ a is primitive $\pmod{2^k p+1}$. Let $d = o(a) \qquad \pmod{2^k p+1}$

$\Rightarrow d = 2^k p \Rightarrow a^{2^k} \not\equiv 1 \pmod{2^k p+1}$

a primitive $\Rightarrow (a, 2^k p+1) = 1$

$\left(\frac{a}{2^k p+1}\right) \equiv a^{\frac{1}{2}((2^k p+1)-1)} \pmod{2^k p+1} \equiv a^{2^{k-1}p} \pmod{2^k p+1} \not\equiv 1 \pmod{2^k p+1}$ (a primitive)

But, the congruence, $x^2 \equiv 1 \pmod{2^k p+1}$ has only two solutions.

$\therefore a^{2^{k-1}p} \equiv -1 \pmod{2^k p+1} \Rightarrow \left(\frac{a}{2^k p+1}\right) = -1$ ✓

(4)

Let $p = 2^n - 1$ prime (i.e. a Mersenne prime) $\therefore n \geq 2$

$(-1)^{\frac{1}{8}(p^2-1)} = \left(\frac{2}{p}\right) \equiv 2^{\frac{1}{2}(p-1)} \pmod{p}$

$\Rightarrow (-1)^{\frac{1}{8}(2^{2n}-2^{n+1})} \equiv 2^{\frac{1}{2}(p-1)} \pmod{p}$

$\therefore$ If $n \geq 3$, then $2^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p} \Rightarrow 2$ is not primitive $\pmod{p}$

In addition, $n = 2 \Rightarrow p = 3$ and 2 is primitive (mod 3)

Let $p = 2^{2^k} + 1$ prime (i.e. a Fermat prime) $\therefore k \geq 0$

$(-1)^{\frac{1}{8}(p^2-1)} = \left(\frac{2}{p}\right) \equiv 2^{\frac{1}{2}(p-1)} \pmod{p}$

$\Rightarrow (-1)^{\frac{1}{8}(2^{2^{k+1}}+2^{2^k+1})} \equiv 2^{\frac{1}{2}(p-1)} (\text{mod } p)$

$\therefore$ If $k \geq 2$, then $2^{\frac{1}{2}(p-1)} \equiv 1 (\text{mod } p) \Rightarrow 2$ is not primitive (mod p)

In addition, $k = 0 \Rightarrow p = 3$ and 2 is primitive (mod 3)   and

$k = 1 \Rightarrow p = 5$ and 2 is primitive (mod 5)

In summary, 3 is the only Mersenne prime that has 2 as a primitive root and 3 and 5 are the only Fermat primes that have 2 as a primitive root. ✓