MATH 542 NUMBER THEORY
Problems to Think About #3
CH. 3, #1-3

Russell Jahn

February 11th, 2014

(1)

p prime, $p \equiv 3 (\text{mod } 4)$

g primitive $(\text{mod } p) \Rightarrow (g,p) = 1$ and $g^{\phi(p)} \equiv 1 (\text{mod } p)$ and $g^d \not\equiv 1 (\text{mod } p)$ for $1 \leq d < \phi(p) = p-1$

Consider $\{g, g^2, ..., g^{p-1}\}$

$(g,p) = 1 \Rightarrow (g^i, p) = 1 \quad \forall i$

Suppose $g^i \equiv g^j (\text{mod } p)$ WLOG, let $1 \leq i \leq j \leq p-1$ $(\therefore 0 \leq j-i \leq p-2)$

$\Rightarrow g^{j-i} \equiv 1 (\text{mod } p) \Rightarrow j = i$ (since g primitive and $j - i \leq p-2$)

$\therefore \{g^i : 1 \leq i \leq p-1\}$ are distinct $(\text{mod } p)$

$\therefore \{g^i : 1 \leq i \leq p-1\} \equiv \{1, 2, ..., p-1\} (\text{mod } p)$ in some order

$\Rightarrow g^i \equiv p-1 \equiv -1 (\text{mod } p)$ for some $i \ni 1 \leq i \leq p-2$ (remembering that $g^{p-1} \equiv 1$)

Now, $g^{p-1} \equiv 1 \Rightarrow g^{\frac{p-1}{2}} \equiv -1$ (since Lagrange's Theorem implies 1 and -1 are the only solutions and $g^{\frac{p-1}{2}} \not\equiv 1$ since g is primitive)

$\Rightarrow g^{\frac{3+4k-1}{2}} \equiv -1$ for some $k \in \mathbb{Z}$

$\Rightarrow g^{1+2k} \equiv -1$ (where $1 + 2k = \frac{p-1}{2}$)

Now, $-g \equiv (-1)(g) \Rightarrow (-g)^{1+2k} \equiv (-1)^{1+2k} g^{1+2k} \equiv (-1)(-1) \equiv 1$

$\therefore (-g)^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$ and $\frac{p-1}{2} < p - 1 = \phi(p)$

$\therefore -g$ is not primitive $(\text{mod } p)$ ✓

(2)

Let p prime and $(a,p) = 1$ let $p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$ be the UPF of $p-1$

$(\Rightarrow)$ a is primitive $(\text{mod } p)$

$\Rightarrow o(a) = p - 1 \ (\text{mod } p)$

Suppose $a^{\frac{p-1}{q_i}} \equiv 1 (\text{mod } p)$ for some q_i $1 \leq i \leq r$

$\Rightarrow o(a) < p - 1 \quad (\Rightarrow \Leftarrow)$

$\therefore a^{\frac{p-1}{q_i}} \not\equiv 1(\text{mod } p) \quad \forall q_i \quad 1 \le i \le r$

$(\Leftarrow) \quad a^{\frac{p-1}{q_i}} \not\equiv 1(\text{mod } p) \quad \forall q_i \quad 1 \le i \le r$

Let $o(a) = d \text{ (mod } p)$

$\Rightarrow d \mid p-1$ and $d \nmid \frac{p-1}{q_i} \quad \forall q_i \quad 1 \le i \le r \quad$ (else $a^{\frac{p-1}{q_i}} \equiv 1(\text{mod } p)$)

$d \mid p-1 \Rightarrow p-1 = ds$ for some $s \in \mathbb{Z}$

$\Rightarrow \frac{ds}{q_i} = \frac{p-1}{q_i} \Rightarrow \frac{s}{q_i} = \frac{\frac{p-1}{q_i}}{d} \notin \mathbb{Z}$

$\Rightarrow s$ contains no powers of q_i in its UPF $\quad \forall i \quad 1 \le i \le r$

$ds = p-1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} \Rightarrow s \mid q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} \Rightarrow s = 1$

$\Rightarrow d = p-1 \Rightarrow a$ is primitive (mod p) $\quad \checkmark$

(3)

I wrote a program on Mathematica to gain insight on a possible conjecture. The program calculates the order (mod p^n) of the first few positive $a \equiv 1(\text{mod } p)$ with $a > 1$ (e.g. $a = 1+p, a = 1+2p$, etc.) for the first few $n = 1, 2, \ldots$.

At first, I made the BIG mistake of running it for just $p = 2$, which seemingly had no discernible pattern, and I began to think the problem was undoable for me. However, by running the program for the first few odd primes, the pattern became clear. Furthermore, in the course of working out the proof for the odd primes, there was nothing in the proof preventing the conjecture from holding for $p = 2$ ...(as long as $j \neq 1$). Upon restudying the output for $p = 2, j \neq 1$, I could see this was the case.

The case of $p = 2, j = 1$ was very difficult. After some study, it became evident that the pattern must depend on the integer l that divides $a-1$ (i.e. $a - 1 = 2l$). After much trial and error, it turned out that the needed information was how large of a power of 2 divides $l+1$.

I then made a conjecture based on the output for this case and proceeded to prove with essentially the same type of proof as in the first case.

Conjecture: For p odd, $j \geq 1$ and $p = 2, j > 1$, we claim, for $a > 1$, $a \equiv 1(\text{mod } p)$,

that $o_n(a) = \text{Max}(1, p^{n-j})$ where j is the largest positive integer $\ni p^j \mid a-1$

Proof: By induction on n we will show:

(1) $o_n(a) = \text{Max}(1, p^{n-j})$ and

(2) $p^{n+1} \nmid a^{o_n(a)} - 1$ if $n \geq j$ (this part is necessary to imply the validity of (1) for $n+1$)

First of all , we note $a \equiv 1(\text{mod } p) \Rightarrow p \mid a-1 \Rightarrow j \geq 1$

and $a = 1 + lp^j$ for some $l \in \mathbb{N} \ni (l, p) = 1$

Base case: $n = 1 \Rightarrow a = 1 + lpp^{j-1} \Rightarrow a \equiv 1(\text{mod } p) \Rightarrow o_1(a) = 1$

$n = 1 \leq j \Rightarrow \text{Max}(1, p^{1-j}) = 1 = o_1(a) \quad \therefore (1)$ is satisfied

Furthermore, $\begin{cases} j = 1 = n \Rightarrow p^{n+1} = p^2 \nmid a-1 \text{ by maximality of } j \\ j > 1 = n \Rightarrow (2) \text{ is vacuously satisfied (a strategy employed by Dr. Fenrick in several of her Sylow proofs)} \end{cases}$

$\therefore$ (1) and (2) are satisfied for $n = 1$

Inductive Hypotheses: Assume, for $m =$ some $n \geq 1$, (1) $o_m(a) = \text{Max}(1, p^{m-j})$ and

(2) $p^{m+1} \nmid a^{o_m(a)} - 1$ if $m \geq j$

(case 1) $j > n \Rightarrow o_n(a) = \text{Max}(1, p^{n-j}) = 1$

We have $a = 1 + lp^j$ where $(l, p) = 1$ for some $l \in \mathbb{N}$

$j > n \Rightarrow j \geq n+1 \Rightarrow a = 1 + lp^{n+1}p^{j-(n+1)} \Rightarrow o_{n+1}(a) = 1 = \text{Max}(1, p^{n+1-j})$

Moreover, $\begin{cases} j = n+1 \Rightarrow p^{n+2} \nmid a - 1 \text{ by maximality of } j \\ j > n+1 \Rightarrow (2) \text{ is vacuously satisfied for } m = n+1 \end{cases}$

$\therefore$ (1) and (2) are satisfied for $m = n+1$

(case 2) $j \leq n \Rightarrow o_n(a) = p^{n-j}$

$\therefore a^{p^{n-j}} = 1 + p^n r$ for some $r \in \mathbb{N} \ni (p, r) = 1$ by inductive hypotheses

$\Rightarrow a^{p^{n+1-j}} = a^{p^{n-j}p} = (1 + p^n r)^p = 1 + (\sum_{i=1}^{p-1} \binom{p}{i} p^{ni} r^i) + p^{np} r^p \quad (*)$

For $1 \leq i \leq p-1$, $\binom{p}{i} = \frac{p(p-1)!}{i!(p-i)!} \in \mathbb{Z}$ with all factors in denominator $< p$ $\Rightarrow p \mid \binom{p}{i}$

$\Rightarrow$ Every term in the Σ is divisible by p^{n+1}

Furthermore, since $np \geq n+1$ (the last term on the right),

we get $p^{n+1} \mid a^{p^{n+1-j}} - 1 \Rightarrow a^{p^{n+1-j}} \equiv 1 (\text{mod } p^{n+1}) \Rightarrow o_{n+1}(a) \mid p^{n+1-j}$

Moreover, $p^{n+1} \nmid a^{p^{n-j}} - 1$ by inductive hypothesis (2) $\Rightarrow p^{n+1} \nmid a^{p^t} - 1 \quad \forall t \leq n-j$

$\Rightarrow o_{n+1}(a) = a^{p^{n+1-j}}$ $\therefore$ (1) is satisfied for $m = n+1$

To show (2) is satisfied for $m = n+1 > j$:

From $(*)$ $a^{p^{n+1-j}} - 1 = pp^n r + (\sum_{i=2}^{p-1} \binom{p}{i} p^{ni} r^i) + p^{np} r^p$

$= p^{n+1}(r + r^p p^{np-(n+1)}) + (\sum_{i=2}^{p-1} \binom{p}{i} p^{ni} r^i) \quad (**)$

Now, $\binom{p}{i} p^{ni} r^i = \frac{p(p-1)!}{i!(p-i)!} p^{ni} r^i \in \mathbb{Z}$

All factors in the denominator are $< p$

$\Rightarrow$ exponent of p in this term is $1+ni$ where $1+ni \geq 1+2n = 1+n+n \geq n+2$ for $2 \leq i \leq p-1$

$\Rightarrow p^{n+2} \mid \sum_{i=2}^{p-1} \binom{p}{i} p^{ni} r^i$

Now, referring to the term on the left of $(**)$,

If $np - (n+1) \geq 1$, then $p^{n+2} \nmid$ this term (since $(r, p) = 1$)

$\Rightarrow p^{n+2} \nmid a^{p^{n+1-j}} - 1$ thus satisfying (2)

However, $np - (n+1) = 0$ only when $p = 2$ and $n = 1$ $(\therefore j = 1$ since $n \geq j)$

But, we excluded the case of $p = 2, j = 1$ in our original hypotheses

$\therefore$ (2) is satisfied for $m = n+1$

$\therefore$ (1) and (2) have been satisfied for $m = n+1$ in all cases

$\therefore$ By induction, in particular, $\quad o_n(a) = \text{Max}(1, p^{n-j})$ for p odd, $\ j \geq 1$ and $p = 2,\ j > 1 \quad \forall n \geq 1 \quad \checkmark$

Conjecture for a formula for $p = 2, j = 1$ is:

When $a = 1 + 2l$ and $l + 1 = 2^k s$ where $(l, 2) = 1$ (since $j = 1$) and $(s, 2) = 1$ (so k is the greatest positive integer such that 2^k divides $l + 1$ then:

$$o_n(a) = \begin{cases} 1, & n = 1 \\ \text{Max}(2, 2^{n-k-1}), & n \geq 2 \end{cases}$$

Pf:

(case 1) $n = 1$

We have $a = 1 + 2l$ where $l \geq 1$ (since $a > 1$), $\ l + 1 = 2^k s,\ (s, 2) = 1,\ (l, 2) = 1$ (since $j = 1$)

$\Rightarrow 2 \mid a - 1 \Rightarrow o_1(a) = 1$

(case 2) $n > 1$

By induction on n, we will show: (1) $o_n(a) = \text{Max}(2, 2^{n-k-1})$

(2) $2^{n+1} \nmid a^{o_n(a)} - 1$ for $n \geq k + 2$

Base case: $n = 2$

Note: l odd $\Rightarrow l + 1$ even $\Rightarrow k \geq 1 \Rightarrow n - k - 1 = 2 - k - 1 \leq 0$

$\therefore a = 1 + 2l = 1 + 2((l + 1) - 1) = 1 + 2 \cdot 2^k s - 2 \Rightarrow 2^2 \nmid a - 1 \ \therefore o_2(a) \neq 1$

But, $a^2 = 1 + 2 \cdot 2l + 2^2 l^2 \Rightarrow 2^2 \mid a^2 - 1 \ \therefore o_2(a) = 2 = \text{Max}(2, 2^{1-k}) = \text{Max}(2, 2^{n-k-1})$

$\therefore$ (1) is satisfied

Moreover, $k + 2 \geq 3 > 2 = n \ \therefore$ (2) is vacuously satisfied

$\therefore$ Base case is satisfied

Inductive hypotheses: Assume for $m =$ some $n \geq 2$ that: (1) $o_m(a) = \text{Max}(2, 2^{m-k-1})$

(2) $2^{m+1} \nmid a^{o_m(a)} - 1$ for $m \geq k + 2$

(case 2a) $2 \leq n < k + 2 \Rightarrow o_n(a) = 2$ and $n + 1 \leq k + 2$

As above, $a - 1 = 2^{k+1} s - 2 = 2(2^k s - 1) \Rightarrow 2^3 \nmid a - 1 \Rightarrow 2^{n+1} \nmid a - 1 \ \therefore o_{n+1}(a) \neq 1$

$a^2 = (1 + 2l)^2 = 1 + 2^2 l(l + 1) = 1 + 2^2 l 2^k s = 1 + 2^{k+2} ls$

$\Rightarrow 2^{k+2} \mid a^2 - 1 \Rightarrow 2^{n+1} \mid a^2 - 1 \ \therefore o_{n+1}(a) = 2 = \text{Max}(2, 2^{n+1-k-1})$

$\therefore$ (1) is satisfied for $m = n + 1$

Also, $\begin{cases} n + 1 < k + 2 \Rightarrow \text{(2) is vacuously satisfied for } m = n + 1 \\ n + 1 = k + 2 \Rightarrow n = k + 1 \Rightarrow a^{o_{n+1}(a)} = a^2 = 1 + ls 2^{k+2} = 1 + ls 2^{n+1} \Rightarrow 2^{n+2} \nmid a^{o_{n+1}} - 1 \\ \qquad\qquad \therefore \text{(2) is satisfied for } m = n + 1 \end{cases}$

$\therefore$ (1) and (2) are satisfied for $m = n + 1$ for (case 2a)

(case 2b) $n \geq k + 2 \Rightarrow o_n(a) = 2^{n-k-1}$

$\Rightarrow a^{2^{n+1-k-1}} = a^{2^{n-k-1} 2} = (1 + 2^n r)^2$ where $(r, 2) = 1$

(since $2^{n+1} \nmid a^{2^{n-k-1}} - 1$ by ind. hyp. (2))

$= 1 + 2 \cdot 2^n r + 2^{2n} r^2 = 1 + 2^{n+1}(r + 2^{n-1} r^2) \quad (***)$

$\Rightarrow 2^{n+1} \mid a^{2^{n+1-k-1}} - 1 \quad \therefore o_{n+1}(a) \mid 2^{n+1-k-1}$

However, by inductive hypothesis (2),

$2^{n+1} \nmid a^{o_n(a)} - 1 = a^{2^{n-k-1}} - 1$

$\Rightarrow 2^{n+1} \nmid a^{2^t} - 1$ for $t \leq n-k-1$

$\therefore\ o_{n+1}(a) = 2^{n+1-k-1} \quad \therefore$ (1) is satisfied for $m = n+1$

Furthermore, from $(***)$, since $n-1 \geq k+1 \geq 2$ and $(r,2) = 1$, we get

$2^{n+2} \nmid a^{2^{n+1-k-1}} - 1 \Rightarrow 2^{n+2} \nmid a^{o_{n+1}(a)} - 1$ and (2) is satisfied for $m = n+1$

$\therefore$ All cases are satisfied for $m = n+1$

$\therefore$ By induction, and in particular, $o_n(a) = \text{Max}(2, 2^{n-k-1})$ for $n \geq 2$

$\therefore$ Conjecture for $p = 2, j = 1$ is proved $\quad \checkmark$