Math 124 Homework 2 Solutions

by Luke Gustafson

Fall 2003

1. First, cancel out the factors of p so that we avoid division by zero:

$$\begin{pmatrix} 2p \\ p \end{pmatrix} = \frac{2p(2p-1)(2p-2)\cdots(1)}{p^2(p-1)^2(p-2)^2\cdots(1)^2}$$

$$= \frac{2p(2p-1)(2p-2)\cdots(p+1)}{p(p-1)(p-2)\cdots(1)}$$

$$= \frac{2(2p-1)(2p-2)\cdots(p+1)}{(p-1)(p-2)\cdots(1)}$$

Now, each factor in the denominator is relatively prime to p, so we can safely reduce modulo p:

$$\begin{pmatrix} 2p \\ p \end{pmatrix} \equiv \frac{2(2p-1)(2p-2)\cdots(p+1)}{(p-1)(p-2)\cdots(1)} \pmod{p}$$

$$\equiv \frac{2(p-1)(p-2)\cdots(1)}{(p-1)(p-2)\cdots(1)} \pmod{p}$$

All factors cancel except the 2, so we conclude $\begin{pmatrix} 2p \\ p \end{pmatrix} \equiv 2 \pmod{p}$.

2a. Expand using the binomial theorem:

$$(1+p)^p \equiv \sum_{i=0}^{p} \begin{pmatrix} p \\ i \end{pmatrix} p^i \pmod{p}$$

$$\equiv 1 + \begin{pmatrix} p \\ 1 \end{pmatrix} p + \begin{pmatrix} p \\ 2 \end{pmatrix} p^2 + \sum_{i=3}^{p} \begin{pmatrix} p \\ i \end{pmatrix} p^i$$

Every term $\begin{pmatrix} p \\ i \end{pmatrix} p^i$ is $\equiv 0 \pmod{p^3}$ for $i \geq 3$, so the sum reduces to

$$\equiv 1 + \begin{pmatrix} p \\ 1 \end{pmatrix} p + \begin{pmatrix} p \\ 2 \end{pmatrix} p^2$$

$$\equiv 1 + p^2 + \left(\frac{p-1}{2}\right) p^3$$

If p is an odd prime, then $\frac{p-1}{2}$ is an integer, and it reduces to $1 + p^2 \pmod{p}$ as desired.

2b. Use induction on n. A direct proof is possible, but it is difficult, as it relies on knowing exactly how many factors of p are in $\binom{p^n}{i}$. In the case $n = 2$, there is nothing to prove. Our base case is $n = 3$, which was shown in part (a). Suppose that the equation holds for some $n \geq 3$.

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

From this, conclude

$$(1+p)^{p^{n-2}} = 1 + p^{n-1} + kp^n$$

for some integer k. Raise both sides to the pth power:

$$(1+p)^{p^{n-1}} = (1 + p^{n-1} + kp^n)^p$$

$$= (1 + p^{n-1}(1+kp))^p$$

Expand this using the binomial theorem:

$$= 1 + \binom{p}{1} p^{n-1}(1+kp) + \sum_{i=2}^{p} \binom{p}{i} p^{i(n-1)}(1+kp)^i$$

Now, for $i \geq 2$ and $n \geq 3$, $i(n-1) \geq n+1$, so all the terms inside the sum are $\equiv 0 \pmod{p^{n+1}}$. Therefore,

$$(1+p)^{p^{n-1}} \equiv 1 + \binom{p}{1} p^{n-1}(1+kp) \pmod{p^{n+1}}$$

$$\equiv 1 + p^n + kp^{n+1} \pmod{p^{n+1}}$$

$$\equiv 1 + p^n \pmod{p^{n+1}}$$

This shows the equation holds for $n+1$, and completes the proof.

2c. $\eta^{p-1} \equiv \epsilon^{(p-1)p^{n-1}} \pmod{p^n}$. Since ϵ is a primitive root mod p, it is relatively prime to p and therefore p^n. Moreover, we have $\varphi(p^n) = (p-1)p^{n-1}$. Using Euler's generalization of Fermat's theorem, we have $\epsilon^{(p-1)p^{n-1}} \equiv \epsilon^{\varphi(p^n)} \equiv 1 \pmod{p^n}$.

2d. $\eta \equiv \epsilon^{p^{n-1}} \equiv \epsilon^{(p-1)(p^{n-2}+p^{n-3}+\cdots+1)+1} \pmod{p}$. Using Fermat's theorem $\epsilon^{p-1} \equiv 1$, so $\epsilon^{(p-1)(p^{n-2}+p^{n-3}+\cdots+1)+1} \equiv \epsilon^{(p-1)(p^{n-2}+p^{n-3}+\cdots+1)} \cdot \epsilon \equiv 1 \cdot \epsilon \pmod{p}$, as desired.

From part (c), we know the order of η is no greater than $p-1$. Now, suppose the order of η is $k < p-1$. Then $\eta^k \equiv 1 \pmod{p^n}$, so $\eta^k \equiv \epsilon^k \equiv 1 \pmod{p}$, which is impossible since ϵ is a primitive root. Therefore, the order of η is exactly $p-1$.

2e. There are exactly $\varphi(p^n) = (p-1)p^{n-1}$ residues mod p^n that are relatively prime to p^n. Furthermore, χ^k is relatively prime to p^n since χ is. Since the order of χ is $(p-1)p^{n-1}$, the powers of χ take on $(p-1)p^{n-1}$ distinct values mod p^n. Thus the powers of χ and the residues of p^n coprime to p^n must be the same set, and the proof is complete.

2f. The proof fails in part (a). One may check that $(1+2)^2 \not\equiv 1+2^2 \pmod{2^3}$. Part (b) relies on this fact to begin the induction, so the rest of the proof fails, too.

To show there is no primitive root χ modulo 8, simply show that each possible χ does not work. Clearly χ must be odd; otherwise $\chi^k \equiv 1$ has no solution, for example.

We check that the order of χ is always less than $\varphi(8) = 4$, which means the powers of χ do not take on all four values 1, 3, 5, 7.

$\chi \equiv 1$ has order 1.
$\chi \equiv 3$ has order 2 since $3^2 \equiv 1$.
$\chi \equiv 5$ has order 2 since $5^2 \equiv 1$.
$\chi \equiv 7$ has order 2 since $7^2 \equiv 1$.
Therefore, there are no primitive roots modulo 8.

3a. Since ϵ is a primitive root, the powers of ϵ take on all non-zero residues as values. Hence the sets $\{\epsilon^0, \epsilon^1, \ldots, \epsilon^{p-2}\}$ and $\{1, 2, \cdots, p-1\}$ are equal mod p. Therefore,

$$\sum_{a=1}^{p-1} a^k \equiv \sum_{n=0}^{p-2} (\epsilon^n)^k$$

which gives the desired result.

3b. We have

$$\begin{aligned}
(\epsilon^k - 1)S &\equiv (\epsilon^k - 1) \sum_{n=0}^{p-2} \epsilon^{nk} \\
&\equiv \sum_{n=0}^{p-2} \epsilon^{nk} \cdot \epsilon^k - \sum_{n=0}^{p-2} \epsilon^{nk} \\
&\equiv \sum_{n=0}^{p-2} \epsilon^{(n+1)k} - \sum_{n=0}^{p-2} \epsilon^{nk} \\
&\equiv \sum_{n=1}^{p-1} \epsilon^{nk} - \sum_{n=0}^{p-2} \epsilon^{nk}
\end{aligned}$$

All the terms cancel except $\epsilon^{(p-1)k} - \epsilon^0$. Using Fermat's theorem, $\epsilon^{(p-1)k} \equiv 1$. Furthermore, $\epsilon^0 \equiv 1$, so we conclude $(\epsilon^k - 1)S \equiv 0 \pmod{p}$.

3c. If $p - 1 \nmid k$, then $\epsilon^k \not\equiv 1 \pmod{p}$ since ϵ is a primitive root. Therefore $\epsilon^k - 1 \not\equiv 0 \pmod{p}$. Since $(\epsilon^k - 1)S \equiv 0$, we must have $S \equiv 0 \pmod{p}$.

3d. Suppose $p - 1|k$. Then $k = i(p - 1)$ for some non-negative integer i. Hence

$$\begin{aligned}\sum_{n=0}^{p-2} \epsilon^{nk} &\equiv \sum_{n=0}^{p-2} (\epsilon^{p-1})^{in} \\ &\equiv \sum_{n=0}^{p-2} 1 \\ &\equiv p - 1\end{aligned}$$

So, $S \equiv -1 \pmod{p}$.