MATH 115, FALL 2010, NOTES ON MULTIPLICATIVE ORDERS OF INTEGERS

MARTIN OLSSON

Throughout p denotes a prime number.

Definition 1. Let a be an integer not divisible by p. The *order* of $a \mod p$ is the least positive integer k for which

$$a^k \equiv 1 \pmod{p}.$$

Lemma 2. *Let a be an integer not divisible by p and let k be the order of a. If s is any nonzero integer such that*

$$a^s \equiv 1 \pmod{p}$$

then $k|s$.

Proof. Let g be the greatest common divisor of s and k, and write

$$g = \alpha s + \beta k$$

with α and β integers. Then

$$a^g \equiv a^{\alpha s + \beta k} \equiv (a^s)^\alpha \cdot (a^k)^\beta \equiv 1 \pmod{p}.$$

Since k was minimal this implies that $g = k$ so $k|s$. □

Lemma 3. *Let a be an integer not divisible by p and let k be the order of a. Then for any integer s, the order of a^s is equal to $k/(s,k)$.*

Proof. By lemma 2, for an integer t we have

$$(a^s)^t = a^{st} \equiv 1 \pmod{p}$$

if and only if $k|st$. Now the condition that $k|st$ is equivalent to the condition that $k/(k,s)$ divides t. Therefore the order of a^s is equal to $k/(k,s)$. □

Lemma 4. *Let a and a' be two integers not divisible by p, and let k (resp. k') be the order of a (resp. a') mod p. Then the order of aa' mod p is equal to $k \cdot k'$.*

Proof. Let k'' denote the order of aa'. Since

$$(aa')^{kk'} = (a^k)^{k'}(a'^{k'})^k \equiv 1 \pmod{p}$$

we have $k''|(kk')$.

On the other hand, the element

$$(aa')^k = a^k a'^k \equiv a'^k \pmod{p}$$

has by lemma 3 order equal to $k''/(k'',k)$. On the other hand also by lemma 3 the order of a'^k is equal to k' since $(k,k') = 1$. Therefore

$$k' | \frac{k''}{(k'',k)},$$

and in particular $k'|k''$. Similarly $k|k''$, and since $(k,k') = 1$ this gives $(kk')|k''$. We conclude that $k'' = kk'$. □

Lemma 5. *Let d be the maximum possible orders among integers a prime to p. Then for any integer a not divisible by p, the order of a divides d.*

Proof. Let b be an element of order d, let k be the order of a, and let $g = (k, d)$. Then a^g has order k/g by lemma 3, and k/g is relatively prime to d. Therefore ba^g has order $d \cdot k/g$ by lemma 4, which by the maximality of d implies that $k/g = 1$. Therefore $k|d$. □

Let d be the maximal order of elements mod p as in lemma 5. Since $a^{p-1} \equiv 1 \pmod{p}$ for every integer a prime to p (Fermat's little theorem), d divides $p - 1$. On the other hand the only way for the equation

$$X^d \equiv 1 \pmod{p}$$

to have $p - 1$ solutions is if $d = p - 1$. We conclude:

Theorem 6. *There exists an integer a prime to p of order $p - 1$.*