Geoffrey Parker - grp352
HW 23: 4.18 - 4.23
M328K
April 19th, 2012

4.18 Theorem. *Let p be a prime and a be an integer. If $(a, p) = 1$, then $\mathrm{ord}_p(a)$ divides $p-1$, that is, $\mathrm{ord}_p(a)|p-1$.*

Proof. Let p be a prime and a be an integer with $(a, p) = 1$. Let $k = ord_p(a)$. By Fermat's Little Theorem we know that $a^{p-1} \equiv 1 \pmod{p}$, so by theorem 4.10 $k \mid p-1$. □

4.19 Exercise. *Compute each of the following without the aid of a calculator or computer.*

1. $512^{372} \pmod{13}$.

2. $3444^{3233} \pmod{17}$.

3. $123^{456} \pmod{23}$.

Solution.

1. We know that $13 - 1 = 12$ and $372 = 31 * 12$, so $ord_{13}(512) \mid 372$.
   Therefore $512^{372} \pmod{13} = 1$.
2. $3444^{3233} \pmod{17}$.
3. $123^{456} \pmod{23}$.

□

4.20 Exercise. *Find the remainder upon division of 314^{159} by 31.*

Solution. □

4.21 Theorem. *Let n and m be natural numbers that are relatively prime, and let a be an integer. If $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$, then $x \equiv a \pmod{nm}$.*

Proof. Let n and m be natural numbers with $(n, m) = 1$. Let a and x be integers with $x \equiv a \pmod{n}$ and $x \equiv a \pmod{m}$. So $n \mid x - a$ and $m \mid x - a$. So by theorem 1.42 $nm \mid x - a$. Therefore $x \equiv a \pmod{nm}$. $\square$

4.22 Exercise. *Find the remainder when 4^{72} is divided by 91 $(= 7 \cdot 13)$.*

Solution. $\square$

4.23 Exercise. *Find the natural number $k < 117$ such that $2^{117} \equiv k \pmod{117}$. (Notice that 117 is not prime.)*

Solution. $\square$