Math 103A Midterm 1 Winter, 2006
Prof. Wavrik

1. Find r, $0 < r < 101$ so that $2^{102} \equiv r \mod (101)$.
[101 is a prime]

$2^{101} \equiv 2 \mod (101)$ by Fermat's Theorem, so $2^{102} \equiv 4 \mod (101)$.

2. Let $a = [3]_{19}$. Show that a has an inverse under multiplication and find the inverse.

$1 \cdot 19 + (-6) \cdot 3 = 1$ so $[-6] = [13]$ is the inverse of $[3]$

3. a. Find a permutation σ in S_5 so that $(1\ 2\ 3)\,\sigma = (1\ 2\ 3\ 4\ 5)$
b. Find a permutation τ in S_5 so that $\tau\,(1\ 2\ 3) = (1\ 2\ 3\ 4\ 5)$

Notice that $(1\ 3\ 2)$ is the inverse of $(1\ 2\ 3)$ so

$\sigma = (1\ 3\ 2)(1\ 2\ 3\ 4\ 5) = (3\ 4\ 5)$

$\tau = (1\ 2\ 3\ 4\ 5)(1\ 3\ 2) = (1\ 4\ 5)$

4. Let a, b, and n be positive integers and p a (positive) prime number
a. Show that if $p \mid ab$ then either $p \mid a$ or $p \mid b$.
b. Show that $(a,n)=1$ and $(b,n)=1$ implies $(ab,n)=1$.

Since p is prime we have (a,p) is either p or 1. If $(a,p)=p$ then $p \mid a$ and we are done. If $(a,p)=1$ then $Aa + Bp = 1$ for some A,B. But then $Aab + Bpb = b$. Since $p \mid Aab$ and $p \mid Bpb$ we have $p \mid b$.

If $(a,n)=1$ we have $Aa + Bn = 1$ for some A,B. Thus $Aab + Bnp = b$. If $g=(ab,n)$ this shows that $g \mid b$. We also have $g \mid n$. So $g \mid (b,n)=1$ We therefore have $g=1$ as desired.

5. Let n be an integer > 1. Fermat's (little) Theorem says that if n is prime then n satisfies the condition:

$$(*)\forall\ x,\ 1<x<n,\ \text{we have } x^{n-1} \equiv 1 \bmod n.$$

Show that the converse is true (i.e. if n satisfies (*) then it must be prime).
[Hint: If n is not prime then show there are zero divisors in $\mathbb{Z}_n$. Show that a zero divisor cannot have an inverse (under multiplication). Observe that $x^{n-1} \equiv 1$ implies x has an inverse in $\mathbb{Z}_n$.]

If n is not prime then $n = ab$ for some $1 < a,b < n$. So a is a zero divisor in $\mathbb{Z}_n$. If $a^{n-1} \equiv 1 \bmod n$ then a has an inverse (namely $c = a^{n-2}$) We have $ab\equiv0$. Multiply by c and we find $b\equiv0$ which cannot happen if $1 < b < n$

Extra Credit Prove or disprove that if there is a permutation σ in S_5 which satisfies $(1\ 2\ 3)\ \sigma\ =\ (1\ 2\ 3\ 4\ 5)$ then σ is unique.

Theorem: σ is unique.

Proof: If $(1\ 2\ 3)\ \sigma\ =\ (1\ 2\ 3\ 4\ 5)$ and $(1\ 2\ 3)\ \tau\ =\ (1\ 2\ 3\ 4\ 5)$ then
$(1\ 3\ 2)(1\ 2\ 3)\ \sigma\ =\ (1\ 3\ 2)(1\ 2\ 3)\ \tau$
so $\sigma\ =\ \tau$