Dr. Marques Sophie
Office 519

Number theory

Fall Semester 2013
marques@cims.nyu.edu

Quizz #3

Due Friday november 22rst in recitation.

Problems:

1. Show that if $n = pq$ is a product of distinct primes and $d \equiv 1 \ mod \ (p-1)(q-1)$ then $A^d \equiv A \ mod \ n$.
2. Show that if p is an odd prime and a is a primitive root mod p, then
$$\left(\frac{a}{p}\right) = -1$$
3. Show that if $n = pq$ with $p < q$, and p, q both prime, then it is not possible for $q-1$ to divide $n-1$. (Hint: If it did, then show that the other factor would have to be too big...)
4. Prove that the equation $x^2 - 3y^2 = 5$ has no solution in integers.
5. Compute $\left(\frac{35}{149}\right)$.

Solution:

1. *Notice that* $(p-1)(q-1) = \phi(n)$. *We know that* $A^{\phi}(n) \equiv 1 \ mod \ n$. *Since* $de \equiv 1 \ mod \ \phi(n)$, *then* $d = 1 + \phi(n)r$, *and the*
$$A^d \equiv A^{1+\phi(n)r} \equiv A \times (A^{\phi})^r \equiv A \ mod \ n$$
.
2. *By Euler's criterion* $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \ mod \ p$. *Since* a *is a primitive root mod* p, *the order of* a *mod* p *is* $p-1$, *so* $x = a^{\frac{p-1}{2}} \not\equiv 1 \ mod \ p$, *since* $\frac{p-1}{2} < p-1$. *But* $x^2 = a^{p-1} \equiv 1 \ mod \ p$, *since* p *is prime,* $a \equiv \pm 1 \ mod \ p$. *So* $x \equiv -1$, *so* $-1 \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$, *so* $\left(\frac{a}{p}\right) = -1$.
3. *Suppose* $q-1|n-1$, *so* $n-1 = (q-1)s$; *since* $n = pq$, *we have* $pq - 1 = qs - s$, *so* $q(s-p) = s-1$, *so* $q|s-1$. *Note that since* $p \geq 2$, $n > q$, *so* $n > q$, *so* $n-1 > q-1$, *so* $s \geq 2$. *But* $q|(s-1)$ *means* $|q| \leq |s-1|$, *i.e.* $s \geq q+1$, *but then* $n-1 = (q-1)s \geq (q-1)(q+1) = q^2 - 1$, *so* $n \geq q^2 > pq = n$, *a contradiction. So* $q-1$ *cannot divide* $n-1$.
Another, shorter, approach: If $n-1 = (q-1)s$, *then since* $n - p = (q-1)p$, *we have* $p-1 = (q-1)(s-p)$, *so* $(q-1)(s-p)$, *so* $(q-1)|(p-1)$, *so* $|q-1| \leq |p-1|$, *which is impossible, since* $p < q$.

4. *Consider the equation modulo* 3*. We get* $x^2 \equiv 5$ *mod* 3*. But* $5 \equiv 2$ *mod* 3 *is not a square modulo* 3*, so this is not possible. Thus the equation has no solutions in integers.*

5.

$$(\frac{35}{149}) = (\frac{149}{35})(-1)^{\frac{149-1}{2}\frac{35-1}{2}} = (\frac{35 \times 4 + 9}{35})(-1)^{74 \times 17} = (\frac{9}{35}) = ((\frac{3}{35}))^2 = 1$$