Math 445 Number Theory

September 20, 2004

Finishing our proof that for n prime, there is an a with $\mathrm{ord}_n(a) = n-1$: we introduce the notation $p^k || N$, which means that $p^k | N$ but $p^{k+1} \not| N$.

For each prime p_i dividing $n-1$, $1 \leq i \leq s$, we let $p_i^{k_i} || n-1$. Then the equation (*) $x^{p_i^{k_i}} \equiv 1 \pmod{n}$ has $p_i^{k_i}$ solutions, while (†) $x^{p_i^{k_i-1}} \equiv 1 \pmod{n}$ has only $p_i^{k_i-1} < p_i^{k_i}$ solutions; pick a solution, a_i to (*) which is not a solution to (†) .

[In particular, $\mathrm{ord}_n(a_i) = p_i^{k_i}$.] Then set $a = a_1 \cdots a_s$. Then a computation yields that, mod n, $a^{\frac{n-1}{p_i}} \equiv a_i^{\frac{n-1}{p_i}} \not\equiv 1$, since otherwise $\mathrm{ord}_n(a_i) | \dfrac{n-1}{p_i}$, and so

$\mathrm{ord}_n(a_i) | \gcd(p_i^{k_i}, \dfrac{n-1}{p_i}) = p_i^{k_i-1}$, a contradiction. So $p_i^{k_i} || \mathrm{ord}_n(a)$ for every i, so $n-1 | \mathrm{ord}_n(a)$, so $\mathrm{ord}_n(a) = n-1$.

This result is fine for theoretical purposes (and we will use it many times), but it is somewhat less than satisfactory for computational purposes; this process of *finding* such an a would be very laborious.

Pythagorian triples: If $a^2 + b^2 = c^2$, then we call (a, b, c) a Pythagorean triple. Their connection to right triangles is well-known, and so it is of interest to know what the triples are! It is fairly straighforward to generate a lot of them (e,g, via $(n+1)^2 = n^2 + (2n+1)$, so any odd square $k^2 = 2n+1$ can be used to build one). But to find them all takes a bit more work:

A Pythagorean triple (a, b, c) is *primitive* if the three numbers share no common factor. This is equivalent, in this case, to $(a, b) = (a, c) = (b, c) = 1$. Then by considering the equation mod 4, we can see that for a primitive triple, c must be odd, a (say) even and b odd. If we then write the equation as $a^2 = c^2 - b^2 = (c+b)(c-b)$, we find that we have factored a^2 in two different ways. Since $a, b+c$ and $b-c$ are all even, we can write $(a/2)^2 = [(c+b)/2]^2[(c-b)/2]^2$ But because $(c+b)/2 + (c-b)/2 = c$ and $(c+b)/2 - (c-b)/2 = b$, $\gcd((c+b)/2, (c-b)/2) = 1$. Then we can apply:

Proposition: If $(x, y) = 1$ and $xy = c^2$, then $x = u^2, y = v^2$ for some integers u, v .

This allows us to write $(c+b)/2 = u^2$ and $(c-b)/2 = v^2$, so $c = u^2 + v^2$ and $b = u^2 - v^2$. Also, $(a/2)^2 = u^2v^2 = (uv)^2$, so $a = 2uv$. So we find that if $a^2 + b^2 = c^2$ is a primitive Pythagorean triple (with the parity information above), then

$$a = 2uv \ , \ b = u^2 - v^2 \ , \text{ and } c = u^2 + v^2 \text{ for some integers } u, v \ .$$

Note that such a triple *is* a Pythagorean triple; these formulas therefore describe *all* primitive Pythagorean triples.