Some answers for the exam questions – Dec 9 2011

1. Since 101 is prime, $a^{100} \equiv 1 \pmod{101}$ for all nonzero a; thus $a^{1000} \equiv 1$ as well.

2. (a) There are 256! permutations. Roughly speaking, $\ln(256!) = 256\ln(256) - n + (\frac{1}{2})\ln(2\pi 256) = 1167.3$ or so, meaning 256! is about 10^{507} . That's a lot!

(b) There are at most 256 permutations of each type. (Only 255 of the second type because we cannot have a=0, and of the third type we are restricted to those power operations which are invertible.) So $|P| < 768$.

(c) Clearly there can be at most 768^2 composites of two, and at most 768^n composites of n, of the elements in P.

(d) The number of permutations that are composites of 100 (or fewer) elements of P is then certainly less than $768 + 768^2 + \ldots + 768^{100} = (768^{101} - 768)/767$ (summing a geometric series). The log of this number is less than $101\log(768) - \log(767)$, about 664.4 — significantly less than the 1167.3 that would be needed to allow for the possibility that we have captured all possible permutations! In fact this same reasoning shows there are permutations that require at least 175 "simple" permutations (and I'm sure that more careful arguments would push that number up even higher).

3. The function $g(m) = m^d$ will invert the cubing operation as long as $3d \equiv 1 \bmod \phi(2047)$. Since $2047 = 23 \cdot 89$, $\phi(2047) = 22 \cdot 88 = 1936 = 3 \cdot 645 + 1$; thus an inverse of 3 is $-645 = 1291$ and we can decrypt a message m by computing $m^{1291} \pmod{2047}$.

(Actually using the Chinese Remainder Theorem, we only need to choose d so that $x^{3d} \equiv 1 \pmod{23}$ and $x^{3d} \equiv 1 \pmod{89}$; so we need $3d \equiv 1 \pmod{22}$ and $3d \equiv 1 \pmod{88}$ for all x; but the latter will imply the former anyway! Since $88 = 3 \cdot 29 + 1$, $3^{-1} = -29 = 59$. Therefore $x \to x^{59}$ is an inverse of the cubing function.

4. By CRT we need $x^2 \equiv 9 \pmod 7$ and $\pmod{13}$. Those moduli are prime so the solutions are precisely the integers x which have $x \equiv 3$ or -3 modulo each of the two primes. We could have $x \equiv +3 \pmod 7$ and $x \equiv +3 \pmod{13}$; those together are equivalent to $x \equiv +3 \pmod{91}$. Similarly $x = -3 \pmod{91}$ is a solution. But we could also have $x \equiv +3 \pmod 7$ and $x \equiv -3 \pmod{13}$; $x \equiv 10 \pmod{91}$ will do this. The remaining case is $x \equiv -10 \pmod{91}$. So the (only) four solutions are $\{3, -3, 10, -10\}$.

5. The p in the definition of ϕ is the same as the p in the cardinality of the field; recall that that prime showed up in our discussion as the *characteristic* of the field: the number of 1's for which $p \cdot 1 = 1+1+\ldots+1 = 0$. So for any element x of the field, $p \cdot x = (p \cdot 1)x = 0x = 0$. As a consequence, $ax = 0$ whenever a is an integer which is a multiple of p.

But if p is prime, then p divides the binomial coefficients $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ when $0 < k < p$. That means that in the expansion of the Binomial Theorem

$$(x+y)^p = \sum_{k=0}^{k=p} \binom{p}{k} x^k y^{p-k}$$

all the terms are zero in F except those corresponding to $k = 0$ and $k = p$, so that $(x + y)^p = x^p + y^p$, which is to say, ϕ preserves sums.

It also obviously preserves products (because multiplication is commutative in a field): $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$.

When $F = Z_p$ itself, then the Fermat theorem asserts that $a^p \equiv a$ for all integers a, i.e. $\phi(a) = a$ for all $a \in Z_p$. In other words, ϕ is the identity function in this case.

When F is a larger field, ϕ is definitely NOT the identity. For example when $F = \{0, 1, a, b\}$ is the field we discussed in class, we must have $\phi(0) = 0$ and $\phi(1) = 1$ but $\phi(a) = a^2 = a + 1 = b$ and similarly $\phi(b) = a$.

6 (a) The point P is of order 3 if $3P = \mathcal{O}$, the identity element of the curve. Well, the most natural way to compute $3P$ is as $2P + P$, so the defining property of being an element of order 3 is that $2P = -P$. But $2P$ is computed by drawing the tangent line at P and finding the other point Q where that line intersects the curve; $2P$ is then defined as the negative of Q. So the point P has order 3 iff $-Q = -P$, i.e., iff the third point of intersection of the line and the curve is ... exactly P again. In other words, the curve has a "triple point" at P – a point of inflection at P.

(b) If (x, y) is a rational point on this elliptic curve, we can find a common denominator Z for x and y to write $x = X/Z$ and $y = Y/Z$ for some other integers X and Y. But then $x^3 + y^3 = 1$ implies $X^3 + Y^3 = Z^3$. As Euler proved, the Fermat conjecture is true for exponent 3, which means that the only solutions in integers to $X^3 + Y^3 = Z^3$ have $X = 0, Y = 0$, and/or $Z = 0$. In our case, Z was chosen as a rational number's denominator, so it is nonzero. If $X = 0$ then $X^3 + Y^3 = Z^3$ implies $Y = Z$ so that $(x, y) = (X/Z, Y/Z) = (0, 1)$. Similarly if $Y = 0$ then $(x, y) = (1, 0)$. So these are the only rational points on this curve.

Observe that this curve then has order exactly 3 (including the point at infinity). That means these are both point of order 3. By part (a), these should also be inflection points. A sketch of the graph (or the use of implicit differentiation) should convince you that this is true.

One can turn the argument backwards: if there is a way to show that the elliptic curve has only these rational points, then Fermat's Last Theorem is true for exponent 3. Indeed, Fermat himself looked at the curve $y^2 = 1 - x^4$; a small bit of algebraic trickery transforms this into an elliptic curve, which allows him to show (by "(infinite) descent") that this curve has no rational points except those with $x = 0$ or $y = 0$. As a consequence, Fermat concluded that there are no two perfect powers that add up to a perfect square – a stronger statement that immediately implies the FLT conjecture is true with exponent 4.

Unfortunately, the corresponding curve for higher exponents is no longer an elliptic curve at all, so it becomes much more difficult to analyze the curve and decide it has only the trivial rational points. The final proof of FLT was related to elliptic curves, but in a very different way.