Some Comments on the homework Math 7770 July 3, 2006

2.7.7 The problem is asking for a counterexample. Many of you noted that the construction that works when p is prime will not work for composite, but this does not prove that there is no other construction that could work.

For instance, let $m = p^2$ for some prime p. Let $F(1) = 1$ and $F(p+1) = 2$. Then we want $f(1) \equiv 1 \bmod p^2$ and $f(p+1) \equiv 2 \bmod p^2$. But if we descend to the modulo p level, this says $f(1) \equiv 1 \bmod p$ and $f(p+1) \equiv f(1) \equiv 2 \bmod p$, impossible. When m is not a power, e.g., if $m = 15$, we let $F(3) = 1$ and $F(6) = 2$ and we have a contradiction when we view any potential f modulo 3.

What is true is that if you restrict F to just mapping residue classes that are relatively prime to m, then the construction given in the text works once you replace $p - 1$ by $\phi(m)$.

In 2.8, many of you are confused about the difference between a quadratic nonresidue and a primitive root.

Claim: A primitive root modulo p is necessarily a quadratic nonresidue modulo that prime.

But the converse is not true. For instance, take $p = 31$. Note that $30 = 2 \cdot 3 \cdot 5$. One can show that 3 is a primitive root by simply calculating the thirty powers of 3 and noting we get all possible residues. Note that $3^5 \equiv 26 \bmod 31$ is a quadratic nonresidue, since $26^{15} \equiv -1 \bmod 31$ but that 26 has order 6 in the multiplicative group, so is not a generator (primitive root). Similarly, $3^{21} \equiv 15 \bmod 31$ is a nonresidue but 15 has order 10.

By the way, the converse is close to being true. Quadratic nonresidues are quite likely to be primitive roots. The prime 31 happens to the worst case, and even here 8 out of the 15 nonresidues are primitive roots. A prime like 23 is more typical: 10 out of 11 nonresidues are primitive roots.

2.8.10 I wrote on most of your papers how the book wanted you to approach this, but let me give one more example. Consider the powers of 2 modulo 13: 2, 4, 8, $2^4 = 3$, $2^5 = 6$, $2^6 = 12$, $2^7 = 11$, $2^8 = 9$, $2^9 = 5$, $2^{10} = 10$, $2^{11} = 7$, $2^{12} = 1$. To solve $x^2 \equiv 10 \bmod 13$ note that x must be of the form 2^a for some a. Thus, the equation is the same as $(2^a)^2 \equiv 2^{10} \bmod 13$ and so $2^{2a-10} \equiv 1 \bmod 13$. But since 2 is a primitive root, the exponent $2a - 10 \equiv 0 \bmod 12$. Thus, $a \equiv 5 \bmod 6$ so a is either 5 or 11. Conclusion: $x \equiv 2^5 \equiv 6 \bmod 13$ or $x \equiv 2^{11} \equiv 7 \equiv -6 \bmod 13$.

2.8.11 Here the text just wanted you to note that the quadratic residues are precisely the even powers of the generator.