Math 139 Solution
Quiz 8 25 April 2003

1. State Fermat's little theorem.

   Solution: Here's the version in the textbook:

   Let p be a prime number. Then

   (a) if a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$;

   (b) for all a, $a^p \equiv a \pmod{p}$.

2. StealthCo Incorporated hires you to consult on a new prime-modulus cryptography system they're implementing. They have decided to use $p = 101$ for their prime.

   (a) One of the StealthCo vice presidents decides he wants to use $e = 32$ for his encryption exponent, and asks you to find the corresponding decryption exponent. What do you tell him?

   Solution: Since 32 is not relatively prime to $p - 1$ (which is 100), he can't use 32 as an encryption exponent. I explain this as gently as I can, and suggest that he choose some other number.

   (b) A second vice president decides she would like to use the encryption key $e = 31$, and asks you to find the corresponding decryption exponent. What do you tell her?

   Solution: Since 31 is relatively prime to 100, we can calculate a decryption exponent, using the extended Euclidean algorithm. The result is

   $$31^{-1} \equiv -29 \equiv 71 \pmod{100}.$$