MATH 180, FINAL

March 19, 2007

Answers

1. (a) Text, p. 79
   (b) Text, p. 69
2. Text, Theorem 6.2
3. Suppose $p \neq 2$ and $p \neq 7$. Then -7 is a square modulo p if and only if $\left(\frac{-7}{p}\right) = 1$, and

$$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{7-1}{2}}\left(\frac{p}{7}\right) = (-1)^{2(p-1)}\left(\frac{p}{7}\right) = \left(\frac{p}{7}\right).$$

   Thus -7 is a square modulo p if and only if p is a square modulo 7, and the squares modulo 7 are $1, 2, 4$. Thus -7 is a square modulo p if and only if $p \equiv 1, 2 \text{ or } 4 \pmod 7$ or $p = 7$.
4. (a) Suppose $N = pq$ with distinct odd primes p, q. By the Chinese Remainder Theorem, the number of solutions of (*) is the product of the number of solutions of $x^2 \equiv a$ modulo p and modulo q. Since (*) has a solution, a is a square modulo p and modulo q, so the equations modulo p and q each have 2 solutions. Therefore (*) has 4 solutions.
   (b) Since $x^2 \equiv a \equiv y^2 \pmod N$, $N \mid (x^2 - y^2) = (x+y)(x-y)$. Since $x \not\equiv \pm y \pmod N$, $N \nmid (x+y)$ and $N \nmid (x-y)$. Hence the gcd $(x+y, N)$ is a *nontrivial* divisor of N, so $(x+y, N) = p$ or q and $N/(x+y, N)$ (or $(x-y, N)$) is the other prime factor.
5. (a) $39/14 = [2, 1, 3, 1, 2]$.
   (b) $2, 3, 11/4, 14/5, 39/14$
   (c) $x = -5, y = 14$
6. The equation $x^5 = 1$ has 1 solution in U_7, and 5 solutions in U_{11}. By the Chinese Remainder Theorem, $x^5 = 1$ has 5 solutions in U_{77}. Exactly 1 of these ($x = 1$) has order 1, and the other 4 must have order 5. Therefore there are 4 elements of U_{77} with order 5.
7. (a) $\alpha = [2, 1, \alpha + 2] = \frac{3\alpha+8}{\alpha+3}$, so $\alpha^2 - 8 = 0$ and $\alpha = \sqrt{8}$.
   (b) The table of convergents is:

		2	1	4	1	4
0	1	2	3	14	17	82
1	0	1	1	5	6	29

so

$$|\tfrac{17}{6} - \sqrt{8}| < \tfrac{1}{6\cdot 29} < .01$$

and 17/6 is the first convergent with this property.

8.

$$\left(\tfrac{41}{101}\right) = \left(\tfrac{101}{41}\right) = \left(\tfrac{19}{41}\right) = \left(\tfrac{41}{19}\right) = \left(\tfrac{3}{19}\right) = -\left(\tfrac{19}{3}\right) = -\left(\tfrac{1}{3}\right) = -1$$

so 41 is *not* a square modulo 101.

9. (a) True
   (b) 40 ($= \varphi(101-1)$)
   (c) 0
   (d) False
   (e) True
   (f) False
   (g) True
   (h) 0
   (i) False