Exam 5 Solutions Math 290 Spring 2014 Name:

Provide brief and logically correct solutions to the following problems:

1. Partition the set $S = \{x \in \mathbb{Z} : 2 \leq x \leq 15\}$ into seven 2-element subsets of the form $\{a, b\}$ where $a < b$ and $ab \equiv 1 \bmod 17$.

Solution: One way to do this is to work out the entire 17×17 multiplication table. Another way is to be on the lookout for products congruent to 1 mod 17. The products must be in the set $\{1, 18, 35, 52, 69, 86, \dots\}$. The numbers in this set factor as follows:

$$1 = 1 \cdot 1$$

$$18 = 2 \cdot 9 = 3 \cdot 6$$

$$35 = 5 \cdot 7$$

$$52 = 4 \cdot 13$$

$$69 = 3 \cdot 23$$

etc.

However one proceeds, the answer is

$$S = \{2, 9\} \cup \{3, 6\} \cup \{4, 13\} \cup \{5, 7\} \cup \{8, 15\} \cup \{10, 12\} \cup \{11, 14\}.$$

2. Let n be a positive integer with prime factorization

$$n = 2^{n_2} 3^{n_3} 5^{n_5} 7^{n_7} 11^{n_{11}} \cdots .$$

Using unique factorization into primes, prove that $\sqrt{n}$ is a rational number if and only if each of the exponents $n_2, n_3, n_5, n_7, n_{11}, \ldots$ is an even number. Do not use negative or fractional exponents in your proof.

Proof: Assume $\sqrt{n}$ is rational. Then $\sqrt{n} = p/q$ for some $p, q \in \mathbb{Z}^+$. Therefore $n = p^2/q^2$ and $q^2 n = p^2$. Write

$$p = 2^{p_2} 3^{p_3} 5^{p_5} 7^{p_7} 11^{p_{11}} \cdots$$

and

$$q = 2^{q_2} 3^{q_3} 5^{q_5} 7^{q_7} 11^{q_{11}} \cdots .$$

Then

$$2^{2q_2+n_2} 3^{2q_3+n_3} 5^{2q_5+n_5} 7^{2q_7+n_7} 11^{2q_{11}+n_{11}} \cdots = 2^{2p_2} 3^{2p_3} 5^{2p_5} 7^{2p_7} 11^{2p_{11}} \cdots .$$

Comparing the exponents, $2q_i + n_i = 2p_i$ for each i, hence $n_i = 2p_i - 2q_i$ for each i, hence each n_i is an even number.

Conversely, assume each n_i is an even number. Write $n_i = 2m_i$ for each i. Then

$$n = 2^{2m_2} 3^{2m_3} 5^{2m_5} 7^{2m_7} 11^{2m_{11}} \cdots ,$$

$$\sqrt{n} = 2^{m_2} 3^{m_3} 5^{m_5} 7^{m_7} 11^{m_{11}} \cdots ,$$

Hence $\sqrt{n}$ is rational.

3. Without using a calculator, find the remainder of 3^{1002} after division by 101.

Solution: Since 101 is a prime number and does not divide 3, by Fermat's Theorem we have $3^{100} \equiv 1 \mod 101$. Raising both sides to the 10^{th} power, this implies $3^{1000} \equiv 1 \mod 101$. Multiplying through by 3^2 yields $3^{1002} \equiv 9 \mod 101$. Hence the remainder is 9.

4. Recall that the order of x mod p is the smallest positive integer k such that $x^k \equiv 1 \bmod p$. Let $S = \{1, 2, 3, 4, 5, 6\}$.

(a) Find the order of each x in S mod 7.

(b) Based on your calculations for (a), find a number g in S having the following property: $\forall x \in S : \exists k \in \mathbb{Z}^+ : x \equiv g^k \bmod 7$.

Solution: Taking each x and forming $x, x^2, x^3, x^4, x^5, x^6$ mod 7, we obtain

$$1, 1, 1, 1, 1, 1\text{: order } 1$$

$$2, 4, 1, 2, 4, 1\text{: order } 3$$

$$3, 2, 6, 4, 5, 1\text{: order } 6$$

$$4, 2, 1, 4, 2, 1\text{: order } 3$$

$$5, 4, 6, 2, 3, 1\text{: order } 6$$

$$6, 1, 6, 1, 6, 1\text{: order } 2.$$

The number g can be any number with order 6. So $g = 3$ and $g = 5$ both work. Using $g = 3$, we have

$$1 \equiv 3^6$$

$$2 \equiv 3^2$$

$$3 \equiv 3^1$$

$$4 \equiv 3^4$$

$$5 \equiv 3^5$$

$$6 \equiv 3^3.$$

5. Define a relation on $\mathbb{Z}$ via $a \sim b$ if and only if $2|(a^2 - b)$. Decide whether or not $\sim$ is an equivalence relation. If it is, describe all the distinct equivalence classes.

Solution: Since $a^2 \equiv a \bmod 2$ for all a using Fermat's theorem or just by thinking about even and odd numbers, we have $a \sim b$ if and only if $a \equiv b \bmod 2$. This is a known equivalence equation whose equivalence classes are [0] and [1]: the even integers and the odd integers.