MIDTERM EXAM REVIEW SOLUTIONS
MATH 115: NUMBER THEORY

Problem 1. There are many possible solutions to this question. To show that S is not well-ordered, we need to show that there is a subset which does not have a least element; it is certainly enough to show that the set S does not have a least element, or what will also suffice, that there exists a decreasing sequence of elements from S.

We consider the elements $1/\sqrt{p}$ for p a prime. By Euclid's theorem, there are infinitely many primes, so the sequence $1/\sqrt{p_n}$ is infinite and strictly decreasing. To conclude, we need to show that $1/\sqrt{p}$ is irrational. Suppose $1/\sqrt{p} = a/b$ where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Then $pa^2 = b^2$, so $p \mid b^2$ and thus since p is prime, $p \mid b$. Let $b = pb'$, so then $pa^2 = (pb')^2 = p^2(b')^2$, hence $a^2 = p(b')^2$, thus $p \mid a^2$ so $p \mid a$. This is a contradiction, since $\gcd(a, b) = 1$.

Problem 2. To find a solution to a congruence modulo $65 = 5 \cdot 13$, we first solve the congruence modulo 5 and modulo 13. Indeed, the congruence

$$x^2 + 1 \equiv 0 \pmod 5$$

has only the solutions $x \equiv \pm 2 \equiv 2, 3 \pmod 5$, and

$$x^2 + 1 \equiv 0 \pmod{13}$$

has only the solutions $x \equiv \pm 5 \equiv 5, 8 \pmod{13}$. Now by the Chinese Remainder Theorem, combining each pair of solutions modulo 5 and 13 gives a solution modulo 65, so there are a total of $2 \cdot 2 = 4$ solutions modulo 65.

A quick application of the CRT gives $x \equiv \pm 8, \pm 18 \equiv 8, 18, 47, 57 \pmod{65}$ as the 4 solutions, but any one of them will do.

Problem 3. We note first that $\gcd(p, q) = 1$ since p, q are distinct primes. Therefore by Fermat's little theorem,

$$p^{q-1} \equiv 1 \pmod q$$

hence also

$$q^{p-1} + p^{q-1} \equiv 1 \pmod q$$

since $q \equiv 0 \pmod q$. Similarly,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod p.$$

Therefore

$$p, q \mid (p^{q-1} + q^{p-1} - 1)$$

and so since $\gcd(p, q) = 1$, we have

$$pq \mid (p^{q-1} + q^{p-1} - 1)$$

hence $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Problem 4. Recall that $\pi(x) = \#\{1 \le a \le x : a \text{ is prime}\}$ counts the number of primes up to a real number $x \in \mathbb{R}_{>0}$, and that

$$\pi(x) \sim \frac{x}{\log x}.$$

Therefore we can estimate

$$\pi(x) \approx \frac{x}{\log x}$$

hence

$$\pi(1000) \approx \frac{1000}{\log 10^3} = \frac{1000}{3\log 10} \approx \frac{1000}{7.5} \approx 133$$

and

$$\pi(100) \approx \frac{10^2}{2\log 10} \approx 20.$$

Therefore the number of primes between 1000 and 100 is

$$\pi(1000) - \pi(100) \approx 133 - 20 = 113.$$

Therefore the probability that such a number is prime is $\approx 113/900$.

Problem 5. Since $(n-2) \mid (2n^2-1)$, we have $\gcd(n-2, 2n^2-1) = n-2$. But since $\gcd(a,c) \mid \gcd(ab,c)$ for all integers a, b, c by unique factorization, we have

$$n-2 = \gcd(n-2, 2n^2-1) \mid \gcd(2(n-2)(n+2), 2n^2-1) = \gcd(2n^2-8, 2n^2-1).$$

Now using the fact that the greatest common divisor only depends on linear combinations, we have by subtracting that

$$\gcd(2n^2-8, 2n^2-1) = \gcd(-7, 2n^2-1) \mid 7$$

so $(n-2) \mid 7$, therefore $n-2 = \pm 1, \pm 7$, which gives $n = -5, 1, 3, 9$, and indeed, each of these checks out.

Alternatively, one can use long division to show that $(2n^2-1)/(n-2) = 2n + 4 + 7/(n-2)$, which is an integer if and only if $(n-2) \mid 7$, as before.

Problem 6. We easily see that $x \equiv 10 \pmod{101}$ is a solution. We now wish to apply Hensel's lemma. We check that

$$f'(10) = 2(10) = 20 \not\equiv 0 \pmod{101^2}$$

so Newton's method applies. We next want to compute $20^{-1} \pmod{101}$, and since

$$20(5) \equiv -1 \pmod{101}$$

we see that $20^{-1} \equiv -5 \pmod{101}$. Therefore by Newton's method,

$$r_1 = r_0 - f(r_0)(-5) = 10 + 5(10^2+1) = 515 \pmod{101^2}$$

is a solution modulo 101^2.