ELEMENTARY NUMBER THEORY

MIDTERM I

(1) Let R be a domain. Give the definitions of units, irreducibles, and primes.

- $u \in R$ is a unit if and only if $u \mid 1$, that is, if and only if $uv = 1$ for some $v \in R$.
- An element $p \in R$ is irreducible if it is a nonunit and if $p = ab$ implies that a or b is a unit.
- An element $p \in R$ is prime if it is a nonunit and if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

(2) State and prove Wilson's Theorem.

Wilson's theorem states that $(p-1)! \equiv -1 \bmod p$ for every prime p. The proof can be found in the notes.

(3) Compute $\gcd(27, 21)$ and the corresponding Bezout representation (you will not get credit for guessing the answer).

$$
\begin{aligned}
27 &= 21 + 6 & \qquad 3 &= 21 - (27 - 21) \cdot 3 \\
21 &= 6 \cdot 3 + 3 & \qquad 3 &= 21 - 6 \cdot 3 \\
6 &= 3 \cdot 2 + 0 & &
\end{aligned}
$$

This shows that $\gcd(27, 21) = 3$ and that $3 = 4 \cdot 21 - 3 \cdot 27$.

(4) Let $n \equiv 7 \bmod 8$ be a natural number. Show that n cannot be written as a sum of three squares.

Every square is congruent to 0, 1, or 4 mod 8. It is now easily checked that the sum of three squares cannot be congruent to 7 mod 8.

(5) Show that $30 \mid (n^5 - n)$ for every $n \geq 1$.

We have $n^5 - n = n(n-1)(n+1)(n^2+1)$. Since n or $n-1$ is even we find $2 \mid (n^5 - n)$. Since on of $n-1$, n, $n+1$ is divisible by 3, we also have $3 \mid (n^5 - n)$. Finally we know $5 \mid n^5 - n$ by Fermat's Little Theorem. Since 2, 3 and 5 are coprime, this shows that $30 \mid n^5 - n$.

(6) Prove that every prime factor of $3x^2 + 1$ is $\equiv 1 \bmod 3$. Then show that there exist infinitely many primes $p \equiv 1 \bmod 3$.

There is a slight problem here: the correct statement is that every odd prime factor of $3x^2 + 1$ is $\equiv 1 \bmod 3$. In fact, $p \mid 3x^2 + 1$ implies $3x^2 \equiv -1 \bmod p$ and $(3x)^2 \equiv -3 \bmod p$. Clearly -3 is a square modulo 2, and we also see that $3 \nmid 3x^2+1$. For primes $p > 3$, the congruence $(3x)^2 \equiv -3 \bmod p$ implies $(\frac{-3}{p}) = +1$, and this holds if and only if $p \equiv 1 \bmod 3$.

In fact, $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{(p-1)/2}(-1)^{(3-1)(p-1)/4}(\frac{p}{3}) = (\frac{p}{3})$, which is $+1$ or -1 according as $p \equiv 1 \bmod 3$ or $p \equiv 2 \bmod 3$.

Now assume that $p_1, \ldots, p_n$ are primes $\equiv 1 \bmod 3$. We will construct a new one by looking at $N = 3(2p_1 \cdots p_n)^2 + 1$. We know that N is odd, hence its prime factors are all $\equiv 1 \bmod 3$. Moreover, $p_j \nmid N$ since $p_j \mid N-1$, hence N is divisible by a prime $p \equiv 1 \bmod 3$ not on the list.

If you look at $N = 3(p_1 \cdots p_n)^2 + 1$ instead, you only know that the odd prime factors are $\equiv 1 \bmod 3$. Luckily it is easy to see that N is not a power of 2: since squares of of numbers are $\equiv 1 \bmod 8$, we have $N \equiv 3 + 1 = 4 \bmod 8$, hence $N/4$ is odd and > 1 since $p_1 \geq 7$.

(7) Assume that $p = a^2 + b^2$ is prime, and that a is odd. Show that $(\frac{a}{p}) = +1$.

Since $p \equiv 1 \bmod 4$ we find $(\frac{a}{p}) = (\frac{p}{a}) = (\frac{a^2+b^2}{a}) = (\frac{b^2}{a}) = +1$.

(8) Is 21 a quadratic residue modulo 101?

$(\frac{21}{101}) = (\frac{101}{21}) = (\frac{-4}{21}) = (\frac{-1}{21}) = +1$ by the first supplementary law. Since 101 is prime, 21 is a quadratic residue modulo 101.

(9) Show that $(\frac{3}{p}) = 1$ for primes $p > 3$ if and only if $p \equiv \pm 1 \bmod 12$.

We have

$$\Big(\frac{3}{p}\Big) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}\Big(\frac{p}{3}\Big) = (-1)^{\frac{p-1}{2}}\Big(\frac{p}{3}\Big).$$

The right hand side can be evaluated easily if the residue class of p mod 12 is known:

- $p \equiv 1 \bmod 12$: $(\frac{3}{p}) = (+1)(+1) = +1$;
- $p \equiv 5 \bmod 12$: $(\frac{3}{p}) = (+1)(-1) = -1$;
- $p \equiv 7 \bmod 12$: $(\frac{3}{p}) = (-1)(+1) = -1$;
- $p \equiv 11 \bmod 12$: $(\frac{3}{p}) = (-1)(-1) = +1$.

This proves the claim.

(10) Assume that $p \equiv 5 \bmod 8$ is prime, and that a is a quadratic residue modulo p.

(a) Show that if $a^{(p-1)/4} \equiv 1 \bmod p$, then $x = a^{(p+3)/8}$ solves the congruence $x^2 \equiv a \bmod p$.

$x^2 \equiv a^{(p+3)/4} \equiv a^{(p-1)/4} \cdot a \equiv a \bmod p$.

(b) If $a^{(p-1)/4} \equiv -1 \bmod p$, then $x \equiv 2a(4a)^{(p-5)/8} \bmod p$ works.

$x^2 \equiv 4a^2(4a)^{(p-5)/4} \equiv 4^{(p-1)/4}a \cdot a^{(p-1)/4} \equiv -2^{(p-1)/2}a \equiv a \bmod p$ because $(\frac{2}{p}) = -1$ for primes $p \equiv 5 \bmod 8$.