ELEMENTARY NUMBER THEORY

MIDTERM 1

(1) Give the precise definitions of
- units: elements dividing 1.
- irreducible elements: nonunits p with only trivial factorizations: if $p = ab$, then a or b is a unit.
- primes: nonunits p with the property that $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Major mistakes: forgetting the condition that p be a nonunit, or sloppy grammar: p is irreducible if $p = ab$ with a or b a unit. This is nonsense, because $4 = 1 \cdot 4$ and 1 is a unit, yet 4 is not irreducible': the condition above must be satisfied for every possible factorization $p = ab$.

(2) Give an example of non-unique factorization in the monoid

$$M = \{1, 4, 7, 10, \ldots\}$$

of natural numbers of the form $3n + 1$, and explain why your example is correct.

In $4 \cdot 25 = 10 \cdot 10$, all factors are irreducible. Thus 100 has at least two distinct factorizations into irreducibles.

If "irreducible" does not show up in your explanation, you will not get full credit.

(3) Consider the statement

$$x^2 \equiv 1 \bmod p \Longrightarrow x \equiv \pm 1 \bmod p. \qquad (*)$$

(a) Show this is true for $p = 6$;

Computing $x^2 \bmod 6$ for $x = 0, 1, \ldots, 5$ shows that $x^2 \equiv 1 \bmod 6$ only if $x \equiv \pm 1 \bmod 6$.
If your proof starts with "Assume that $x \equiv 1 \bmod 6$", you will not get any credit since you assumed what you were supposed to prove.

(b) Show this is true if p is a prime;

Assume that $x^2 \equiv 1 \bmod p$. Then $p \mid (x^2 - 1) = (x - 1)(x + 1)$, and since p is prime, this implies $p \mid (x-1)$ or $p \mid (x+1)$. Thus $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

(c) Give an example that shows $(*)$ is not true in general.

Just observe that $3^2 \equiv 1 \bmod 8$ or $4^2 \equiv 1 \bmod 15$.

(4) Show that there are infinitely many primes of the form $p \equiv 3 \bmod 4$.

Let $p_1 = 3, \ldots, p_n$ be primes $\equiv 3 \bmod 4$, and consider $N = 4p_1 \cdots p_n - 1$. Since $N \equiv 3 \bmod 4$, N contains at least one prime factor $p \equiv 3 \bmod 4$. If we had $p = p_i$, then $p \mid N$ and $p \mid (N+1)$, leading to the contradiction $p \mid 1$.

(5) Let $n \equiv 6 \bmod 7$ be a positive integer. Show that n cannot be written as a sum of five sixth powers.

By Fermat's Little Theorem, we have $a^6 \equiv 1 \bmod 7$ if $7 \nmid a$, and of course $a^6 \equiv 0 \bmod 7$ if $7 \mid a$. Thus $n = a^6 + b^6 + c^6 + d^6 + e^6 \equiv 5, 4, 3, 2, 1, 0 \bmod 7$ according as none, one, $\ldots$, five of the numbers $a, \ldots, e$ are divisible by 7. In particular, no integer $\equiv 6 \bmod 7$ can be written as the sum of five sixth powers.

(6) Apply the Euclidean algorithm to the pair $a = 204$ and $b = 85$, and compute a Bezout presentation of the gcd.

$$\begin{aligned} 204 &= 2 \cdot 85 + 34, \\ 85 &= 2 \cdot 34 + 17, \\ 34 &= 2 \cdot 17. \end{aligned}$$

Thus $\gcd(204, 85) = 17$.

For the Bezout presentation, compute

$$17 = 85 - 2 \cdot 34 = 85 - 2 \cdot (204 - 2 \cdot 85) = 5 \cdot 85 - 2 \cdot 204.$$

If you gave the correct Bezout presentation without computing it, you did non get full credit.

(7) Let p be an odd prime, and assume that $p = e^2 - 2f^2$ for integers e and f. Use Fermat's Little Theorem to prove $2^{(p-1)/2} \equiv 1 \bmod p$ for all such primes.

The only really tricky one. We have $p = e^2 - 2f^2$ and need to prove a congruence modulo p. Thus we start with $e^2 \equiv 2f^2 \bmod p$. Since we need to prove something about $2^{(p-1)/2}$, we raise it to the $\frac{p-1}{2}$-th power and find $e^{p-1} \equiv 2^{(p-1)/2} f^{p-1} \bmod p$. Now $p \nmid ef$, since $p \mid e$ or $p \mid f$ would imply $p \mid e$ and $p \mid f$, hence $p^2 \mid e^2 - 2f^2 = p$: contradiction. But then Fermat's Little Theorem gives the claim.

(8) Give an example showing that cancellation in congruences is not allowed in general.

Simply take $2 \equiv 6 \bmod 4$ and cancel 2: this gives the false congruence $1 \equiv 3 \bmod 4$.

I did not really like examples like $0 \equiv 4 \bmod 4$ and cancelling 4, since $4 \equiv 0 \bmod 4$ and dividing through by 0 is generally a bad idea.

(9) Explain how to solve $x^2 + y^2 = z^2$ in integers (give all the details; proofs are not required).

See the notes.

(10) Let p be an odd prime number. Find all natural numbers $x, y \in \mathbb{N}$ with $x^2 = y^2 + p$.

Write the equation as $p = x^2 - y^2 = (x-y)(x+y)$. Since p is irreducible, and since we only want positive solutions, the only possibility is $x - y = 1$ and $x + y = p$, which gives $x = \frac{p+1}{2}$ and $y = \frac{p-1}{2}$.