Midterm 1 Review

Tim Smits

1. Find all integer solutions to the equation $147x + 258y = 369$.
2. (a) Prove that if $a^n - 1$ is prime, that n is prime and $a = 2$.
   (b) Prove that if $a^n + 1$ is prime, that $n = 2^k$ for some k and a is even.
3. Show that $x^3 + y^3 + z^3 = 400$ has no integer solutions.
4. Show that $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ is an integer for all $n \in \mathbb{Z}$.
5. Let a, b be integers with $a, b > 1$.
   (a) Prove that $\gcd(a^2, b^2) = \gcd(a, b)^2$.
   (b) Prove that $\gcd(ka, kb) = k \cdot \gcd(a, b)$ for any integer $k \geq 1$.
   (c) Show that if $(a^2 - b^2) \mid (a^2 + b^2)$ for some integers a, b, that $(a^2 - b^2) \mid 2\gcd(a, b)^2$.
   (d) Use part (c) to show that there are no integers $a, b > 1$ such that $(a^2 - b^2) \mid (a^2 + b^2)$.
6. Let $p > 2$ be a prime. Show that $x^2 \equiv 1 \bmod p^n$ has two solutions for all $n \geq 1$.

Hints

2. Recall the factorizations of $x^n - 1$ and $x^n + 1$ from homework 1.
3. Work mod 9.
4. Turn this into a divisibility condition and then use modular arithmetic.

5d. Reduce to the case where a, b are relatively prime.

6. Show that a solution of $x^2 \equiv 1 \bmod p^{n+1}$ gives a solution to $x^2 = 1 \bmod p^n$, and then induct.

Solutions

1. Running the Euclidean algorithm,

$$
\begin{aligned}
258 &= 147 \cdot 1 + 111 \\
147 &= 111 \cdot 1 + 36 \\
111 &= 36 \cdot 3 + 3 \\
36 &= 3 \cdot 12 + 0
\end{aligned}
$$

which says $\gcd(147, 258) = 3$. After back substituting, we find that $(-7, 4)$ is one solution to $147x + 258y = 3$, so $(-861, 492)$ is a solution to $147x + 258y = 369$. An arbitrary solution is then of the form $x = -861 + 86k$, $y = 492 - 49k$ for $k \in \mathbb{Z}$.

2. (a) Recall that $a^n - 1 = (a-1)(a^{n-1} + \ldots + 1)$. If $a \neq 2$, then $a - 1 > 1$ so $a^n - 1$ has a non-trivial divisor. If $n = ab$ with $1 < a, b < n$, then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)(2^{ab-a} + \ldots + 1)$ has $2^a - 1$ as a non-trivial divisor. Therefore, for $a^n - 1$ to be prime, n must be prime and $a = 2$.

   (b) Recall that for n odd, we have $a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \ldots + 1)$. Write $n = 2^k \ell$ for some k, ℓ with ℓ odd. If $\ell > 1$, we have $a^n + 1 = (a^{2^k})^\ell + 1$ is divisible by $a^{2^k} + 1 > 1$. If a is odd, then a^{2^k} is also odd for any k, so $a^{2^k} + 1$ is even, and therefore divisible by 2. Therefore, for $a^n + 1$ to be prime, n must be a power of 2 and a must be even.

3. Suppose that $x^3+y^3+z^3 = 400$ had an integer solution. Working mod 9, this says $x^3+y^3+z^3 \equiv 4 \bmod 9$. The cubes mod 9 are $0, 1, 8$, which are the same as $-1, 0, 1 \bmod 9$. This tells us that the possible values of $x^3+y^3+z^3 \bmod 9$ are $0, 1, 2, 3, 6, 7, 8$. Therefore, since $x^3+y^3+z^3 = 400$ has no solutions mod 9, it has no integer solutions.

4. Putting everything over a common denominator, we wish to show that $\frac{3n^5+5n^3+7n}{15}$ is an integer, or equivalently, that $15 \mid 3n^5 + 5n^3 + 7n$ for all n. It's sufficient to show that this expression is divisible by 3 and by 5. Mod 3, we have $3n^5 + 5n^3 + 7n \equiv 2n^3 + n \bmod 3$. Plugging in $n \equiv 0, 1, 2 \bmod 3$ into $2n^3 + n$ yields $0, 3, 18$, which shows that $2n^3 + n \equiv 0 \bmod 3$, i.e. $3 \mid 3n^5 + 5n^3 + 7n$. Similarly, mod 5 we have $3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n \bmod 5$. Plugging in $n \equiv -2, -1, 0, 1, 2 \bmod 5$ into $3n^5 + 5n^3 + 7n$ yields $-100, -5, 0, 5, 100$, so that $3n^5 + 2n \equiv 0 \bmod 5$. This says $5 \mid 3n^5 + 5n^3 + 7n$, so we're done.

5. (a) See the week 3 discussion notes.

   (b) Let $d = \gcd(a, b)$ and $d' = \gcd(ka, kb)$. Since $d \mid a$ and $d \mid b$, we have $kd \mid ka$ and $kd \mid kb$, so $kd \mid d'$. By Bezout's lemma, we can write $ax + by = d$ for some $x, y \in \mathbb{Z}$. Multiplying by k says $kax + kby = kd$. Since $d' \mid ka$ and $d' \mid kb$, this says $d' \mid kd$, so $kd = d'$.

   (c) Suppose that $a^2 - b^2 \mid (a^2 + b^2)$. Then since $a^2 - b^2 \mid (a^2 - b^2)$, this says $a^2 - b^2$ divides $(a^2 + b^2) + (a^2 - b^2) = 2a^2$ and $a^2 - b^2$, divides $(a^2 + b^2) - (a^2 - b^2) = 2b^2$. Therefore, $a^2 - b^2 \mid \gcd(2a^2, 2b^2) = 2\gcd(a, b)^2$ by parts (a) and (b).

   (d) Suppose that $a^2 - b^2 \mid (a^2 + b^2)$, so we can write $(a^2 - b^2)k = a^2 + b^2$ for some k. If $\gcd(a, b) = d > 1$, we can write $a = dm$ and $b = d\ell$ for some m, ℓ. Plugging in says $d^2(m^2 - \ell^2)k = d^2(m^2 + \ell^2)$, so $m^2 - \ell^2 \mid (m^2 + \ell^2)$. By homework 2, $\gcd(m, \ell) = 1$, and by part (c), $(m^2 - \ell^2) \mid 2$. This says $m^2 - \ell^2 = 1$ or $m^2 - \ell^2 = 2$. In the first case, we have $(m - \ell)(m + \ell) = 1$, which would mean $m - \ell = 1$ and $m + \ell = 1$. This has no solutions with both m, ℓ positive. Therefore, $(m - \ell)(m + \ell) = 2$, so we must have $m - \ell = 1$ and $m + \ell = 2$. However, this means $2m = 3$, which has no integer solutions. Therefore, there are no such a, b with $a^2 - b^2 \mid (a^2 + b^2)$.

6. We prove this by induction. For the base case, suppose that $x^2 \equiv 1 \bmod p$. Then $p \mid (x^2 - 1) = (x + 1)(x - 1)$, so by Euclid's lemma, we have $p \mid (x + 1)$ or $p \mid (x - 1)$, i.e. $x \equiv \pm 1 \bmod p$. Now suppose that $x^2 \equiv 1 \bmod p^n$ only has solutions $x \equiv \pm 1 \bmod p^n$ for some

n. Note that $\pm 1 \bmod p^{n+1}$ are solutions to $x^2 \equiv 1 \bmod p^{n+1}$. We now show that these are the only solutions. Suppose that $x^2 \equiv 1 \bmod p^{n+1}$: this means that $x^2 = 1 + p^{n+1}k$ for some k, which means that $x^2 \equiv 1 \bmod p^n$. By assumption, this means that $x \equiv \pm 1 \bmod p^n$, so that $x = \pm 1 + p^n \ell$ for some ℓ. Squaring, we find $x^2 = (\pm 1 + p^n \ell)^2 = 1 + 2p^n \ell + p^{2n}\ell^2$. Taking this mod p^{n+1}, we have $1 \equiv x^2 \equiv 1 + 2p^n \ell \bmod p^{n+1}$. This says $2p^n \ell \equiv 0 \bmod p^{n+1}$, i.e. $p^{n+1} \mid 2p^n \ell$. Since $p > 2$, this means $p \mid \ell$, so that $\ell = pm$ for some m. This says $x = \pm 1 + p^{n+1}m$, which then tells us that $x \equiv \pm 1 \bmod p^{n+1}$ as desired. Therefore by induction, the only solutions to $x^2 \equiv 1 \bmod p^n$ are $x \equiv \pm 1 \bmod p^n$.