

MAT 311: Number Theory

Spring 2008

Solutions to HW1

- (a) Prove that if n is odd, $n^2 - 1$ is divisible by 8.
If n is odd, $n = 2k + 1$ for some integer k . Then $n^2 - 1 = 4k(k + 1)$. But since k and $k + 1$ are consecutive integers, one of them has to be even, thus $k(k + 1)$ is even, say it is $2s$ for some integer s . Thus $n^2 - 1 = 4 \cdot 2s = 8s$. So $8 | n^2 - 1$. \square
(b) Prove that $4 \nmid n^2 + 2$ for any integer n .
 n is congruent to either 0, 1, 2 or 3 (mod 4). So n^2 is congruent to either 0, $1^2 = 1$, $2^2 \equiv 0$ or $3^2 \equiv 1$ (mod 4). Hence $n^2 + 2$ is congruent to 2 or 3 (mod 4). But $4 | n^2 + 2$ iff $n^2 + 2 \equiv 0$ (mod 4). This completes the proof. \square
- Using induction show that $\sum_{i=1}^k 3i^2 - 3i + 1 = k^3$.
Argue by induction on k : The statement is true for $k = 1$, since $3 \cdot 1^2 - 3 \cdot 1 + 1 = 1^3$. Now assume that the statement holds for k . We will show that it holds for $k + 1$, that is $\sum_{i=1}^{k+1} 3i^2 - 3i + 1 = (k + 1)^3$. Indeed: $\sum_{i=1}^{k+1} 3i^2 - 3i + 1 = \{3(k + 1)^2 - 3(k + 1) + 1\} + \sum_{i=1}^k 3i^2 - 3i + 1 = 3k^2 + 3k + 1 + k^3 = (k + 1)^3$, as required.
- Find a parametrization of the rational points on the hyperbola $x^2 - 2y^2 = 1$, starting from the point $(3, 2)$.
If (a, b) is any other rational point on the curve, then the line $y = m(x - 3) + 2$ with $m = \frac{2-b}{3-a}$ will pass through both $(3, 2)$ and (a, b) . (Note that this excludes the exceptional case when $a = 3$ -because $m = \infty$ is then not defined- but if $a = 3$, then b has to be ± 2 , that is, we only omit the single point $(3, -2)$. This is OK, because **ALL** the other rational points on the curve are obtained by considering lines $y = m(x - 3) + 2$ through $(3, 2)$ and intersecting them with our curve.) Observe in passing that m is a rational number. Now, we need to find the coordinates of (a, b) in terms of m to give a parametrization of the curve. So we have to solve intersect the curve with the line: $y = m(x - 3) + 2$ implies that $0 = x^2 - 2y^2 - 1 = x^2 + (m(x - 3) + 2)^2 - \{x^2 - 9\} - 2\{m^2(x - 3)^2 + 4m(x - 3)\} = (x - 3)\{(1 - 2m^2)x + (6m^2 - 8m + 3)\}$. Note that the factor $(x - 3)$ comes out for free, because the point $(3, 2)$ is on the curve. The root of the other factor will give us the x -coordinate of the second intersection point, namely a . So we want to solve $(1 - 2m^2)x + (6m^2 - 8m + 3) = 0$ for x . Of course this gives $x = \frac{6m^2 - 8m + 3}{2m^2 - 1}$, but we have to check that the denominator is nonzero. Indeed $2m^2 - 1 = 0$ iff $m = \pm 1/\sqrt{2}$ which is irrational, therefore not accepted. A straight-forward calculation shows: $y = -\frac{4m^2 - 6m + 2}{2m^2 - 1}$. So all the rational points (a, b) on the curve (except $(3, -2)$) are given by $\{(\frac{6m^2 - 8m + 3}{2m^2 - 1}, -\frac{4m^2 - 6m + 2}{2m^2 - 1}) : m \in \mathbb{Q}\}$. Conversely, any point in the latter set is a rational point, because the coordinates are rational numbers. Therefore, those are **precisely** the rational points on our curve (again, except $(3, -2)$). If you want, you can put $m = s/t$, $s, t \in \mathbb{Z}$, and get $\{(\frac{6s^2 - 8st + 3t^2}{2s^2 - t^2}, -\frac{4s^2 - 6st + 2t^2}{2s^2 - t^2}) : s, t \in \mathbb{Z}\}$. The last expression has the advantage that putting $t = 0$, which corresponds to $m = \infty$, gives us back the missing hidden point $(3, -2)$. \square
- Prove that any positive integer of the form $3k + 2$ has a prime factor of the same form.
We know that every positive integer can be written as a factor of prime numbers. Given a positive integer $n = 3k + 2$ for some k . The prime factors of n are either of the form $3m, 3m + 1$ or $3m + 2$. Now assume, for a contradiction, that none of those primes are of the form $3m + 2$. If there is a prime factor of the form $3m$ -btw, it has to be 3- then this means $n = 3k + 2$ is divisible by 3, which is impossible ($3 | 3k$ but $3 \nmid 2$). Thus, all factors have to be of the form $3m + 1$. But any such two numbers is of the same form, hence (by induction) the whole product, namely $n = 3k + 2$ is of the form $3m + 1$, again a contradiction. This completes the proof. \square