Homework 2

- Please submit your answers to all questions.
- We will mark your answers to 3 questions.
- We will provide you with full solutions to all questions.

1. Prove that if $a \in \mathbb{Z}$, then $4 \nmid a^2 + 1$.

   Proof. Assume $a \in \mathbb{Z}$. Then we have two cases: a is even or a is odd.

   - Case 1: If a is even, then $a = 2k$ for some $k \in \mathbb{Z}$. This implies $a^2 + 1 = 4k^2 + 1$. Since $k^2 \in \mathbb{Z}$, we conclude that $4 \nmid (a^2 + 1)$.
   - Case 2: If a is even, then $a = 2k + 1$ for some $k \in \mathbb{Z}$. This implies $a^2 + 1 = 4k^2 + 4k + 2 = 4(k^2 + k) + 2$. Since $k^2 + k \in \mathbb{Z}$, we conclude that $4 \nmid (a^2 + 1)$.

   $\square$

2. Prove that if $k \in \mathbb{Z}$ then $3|k(2k + 1)(4k + 1)$.

   Proof. We do the Euclidean division of k by 3 so we write $k = 3q + r$ for some $q, r \in \mathbb{Z}$ with $r \in \{0, 1, 2\}$. We then argue by cases.

   - Case 1: if $r = 0$, then $k = 3q$ for some $q \in \mathbb{Z}$. This means that $k(2k+1)(4k+1) = 3q(2k+1)(4k+1)$ so $k(2k+1)(4k+1)$ is a multiple of 3 since $q(2k + 1)(4k + 1)$ is an integer.
   - Case 2: if $r = 1$, then $k = 3q + 1$ for some $q \in \mathbb{Z}$. This implies that $2k+1 = 3(2q+1)$ which implies $k(2k+1)(4k+1) = 3 \cdot k(2q+1)(4k+1)$. Thus, $k(2k + 1)(4k + 1)$ is a multiple of 3 since $k(2q + 1)(4k + 1)$ is an integer.
   - Case 3: if $r = 2$, then $k = 3q + 2$ for some $q \in \mathbb{Z}$. In this case, we see that $4k+1 = 3(4q+3)$, that is, $k(2k+1)(4k+1) = 3 \cdot 3 \cdot k(2k+1)(4q+3)$. Thus, $k(2k + 1)(4k + 1)$ is a multiple of 3 since $k(2k + 1)(4q + 3)$ is an integer.

   $\square$

3. Let $n \in \mathbb{Z}$.

   a) Show that if $3 \mid n$ and $4 \mid n$, then $12 \mid n$.

   b) Use the previous part to show that if $n > 3$ is a prime, then $n^2 \equiv 1 \pmod{12}$.

   Proof. Let $n \in \mathbb{Z}$.

Homework 2

a) Assume that $3 \mid n$ and $4 \mid n$. This means that $n = 3k$ and $n = 4\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore we see that $4\ell = 3k$, which implies that $\ell = 3(k-\ell)$. Using this, we get $n = 4\ell = 4(3(k-\ell)) = 12(k-\ell)$. Hence, since $k - \ell \in \mathbb{Z}$, we see that $12 \mid n$.

b) Assume that $n > 3$ is prime. Then we know that n is odd, that is, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 - 1 = 4k^2 + 4k$, which implies that $4 \mid (n^2 - 1)$. So, using part a), we see that it suffices to show that $3 \mid (n^2 - 1)$. Since $n > 3$ is prime, we know that $3 \nmid n$. Thus, we can prove this using cases.

- Case 1: Let $n = 3\ell + 1$ for some $\ell \in \mathbb{Z}$. Then $n^2 - 1 = 9\ell^2 + 6\ell = 3(3\ell^2 + 2\ell)$ is divisible by 3.
- Case 2:Let $n = 3\ell+2$ for some $\ell \in \mathbb{Z}$. Then $n^2-1 = 9\ell^2+12\ell+3 = 3(3\ell^2 + 4\ell + 1)$ is divisible by 3,

which finishes the proof.

□

4. Let $n \in \mathbb{Z}$. Prove that if $n^3 + n^2 - n + 3$ is a multiple of three, then n is a multiple of three.

Proof. Let $n \in \mathbb{Z}$. We prove this statement using contrapositive. Assume that $3 \nmid n$, then we want to show that $3 \nmid (n^3 + n^2 - n + 3)$.

Since $3 \nmid n$, we see that we have 2 cases. $n = 3q + 1$, or $n = 3q + 2$ for some $q \in \mathbb{Z}$.

- Case 1: $n = 3q + 1$. In this case, we see that

$$\begin{aligned} n^3 + n^2 - n + 3 = n^3 - n + n^2 + 3 &= n(n^2 - 1) + n^2 + 3 \\ &= (n-1)n(n+1) + n^2 + 3 \\ &= 3(qn(n+1) + 1) + (3q+1)^2 \\ &= 3(qn(n+1) + 1 + 3q^2 + 2q) + 1. \end{aligned}$$

  Hence, since $qn(n+1)+1+3q^2+2q \in \mathbb{Z}$, we see that $3 \nmid (n^3+n^2-n+3)$.

- Case 2: $n = 3q + 2$. In this case, we see that

$$\begin{aligned} n^3 + n^2 - n + 3 = n^3 - n + n^2 + 3 &= n(n^2 - 1) + n^2 + 3 \\ &= (n-1)n(n+1) + n^2 + 3 \\ &= 3((n-1)n(q+1) + 1) + (3q+2)^2 \\ &= 3((n-1)n(q+1) + 1 + 3q^2 + 4q) + 1. \end{aligned}$$

  Hence, since $(n-1)n(q+1) + 1 + 3q^2 + 4q \in \mathbb{Z}$, we see that $3 \nmid (n^3 + n^2 - n + 3)$.

Therefore in both cases, we see that if $3 \nmid n$, then $3 \nmid (n^3+n^2-n+3)$. Hence, the result follows. $\square$

5. Let $x \in \mathbb{R}$. Then, prove that $x^2 + |x-6| > 5$.

Proof. We use proof by cases. First, let $x \in \mathbb{R}$.

- Case 1: $x > 6$: In this case we see that $|x-6| = x-6$. Hence we see that for $x > 6$, we have $x-6 > 0$. Moreover, for $x > 6$, multiplying this inequality by x and 6, we conclude $x^2 > 6x > 36$, that is $x^2 > 36$. Therefore, combining $x-6>0$ with $x^2 > 36$, we get $x^2 + x - 6 > 36$.
- Case 2: $x \leq 6$. In this case we see that $|x-6| = 6-x$. Thus, $x^2 + |x-6| = x^2 - x + 6 = (x-\frac{1}{2})^2 + \frac{23}{4} > \frac{20}{4} = 5$ since $(x-\frac{1}{2})^2 \geq 0$ for all $x \in \mathbb{R}$. Hence we see that for $x \leq 6$, $x^2 - x + 6 > 5$. Therefore in both cases, we see that $x^2 + |x-6| > 5$.

$\square$

6. Let $x, y \in \mathbb{Z}$. Prove that

$$3 \nmid (x^3+y^3) \text{ if and only if } 3 \nmid (x+y).$$

Proof. Let $x, y \in \mathbb{Z}$. We see that this is a biconditional statement. We will prove each implication in turn.

- **Proof of $3 \nmid (x^3+y^3)$ implies $3 \nmid (x+y)$:** We prove the contrapositive. Assume $3 \mid (x+y)$. Then we know that $(x+y) = 3k$ for some $k \in \mathbb{Z}$. Thus, $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = 27k^3$. This implies that $(x^3+y^3) = 27k^3 - 3x^2y - 3xy^2 = 3(9k^3 - x^2y - xy^2)$. Since $(9k^3 - x^2y - xy^2) \in \mathbb{Z}$ we see that $3 \mid (x^3+y^3)$
- **Proof of $3 \nmid (x+y)$ implies $3 \nmid (x^3+y^3)$:** Assume that $3 \nmid (x+y)$. Then, we have two cases, $(x+y) = 3k+1$ or $(x+y) = 3k+2$ for some $k \in \mathbb{Z}$.
  - Case 1: $(x+y) = 3k+1$ for some $k \in \mathbb{Z}$. Then we see that $(x^3+y^3) = (x+y)^3 - 3(x^2y+xy^2) = 27k^3 + 27k^2 + 9k + 1 - 3(x^2y+xy^2) = 3(9k^3+9k^2+3k-x^2y+xy^2)+1$. Since $(9k^3+9k^2+3k-x^2y+xy^2) \in \mathbb{Z}$, we see that $3 \nmid (x^3+y^3)$.
  - Case 2: $(x+y) = 3k+2$ for some $k \in \mathbb{Z}$. Then we see that $(x^3+y^3) = (x+y)^3 - 3(x^2y+xy^2) = 27k^3+54k^2+36k+8-3(x^2y+xy^2) = 3(9k^3+18k^2+12k-x^2y+xy^2)+1$. Since $(9k^3+18k^2+12k-x^2y+xy^2) \in \mathbb{Z}$, we see that $3 \nmid (x^3+y^3)$.

$\square$

Homework 2

7. **Bézout's identity**: Let $a, b \in \mathbb{Z}$ such that a and b are not both zero. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

   For example, for $a = 5$ and $b = 7$, we see $\gcd(a, b) = 1$ and we can take $x = 10$ and $y = -7$.

   Now, let $a, b, k \in \mathbb{Z}$ and assume that a, b are not both zero. Then, using Bézout's identity, show that if $k \nmid \gcd(a, b)$, then $k \nmid a$ or $k \nmid b$.

   Proof. We are going to prove this statement using contrapositive. Let $a, b, k \in \mathbb{Z}$ and assume that a, b are not both zero. Moreover, assume that $k \mid a$ and $k \mid b$. This means that $a = km$ and $b = kn$ for some $n, m \in \mathbb{Z}$. We also know that by Bézout's identity, we know that there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. Hence, combining these equations we get $kmx + kny = k(mx + ny) = \gcd(a, b)$. Therefore, since $mx + ny \in \mathbb{Z}$, we get $k \mid \gcd(a, b)$.

   $\square$