CSE 20: Assignment Set 2

1. Show that $a^2 + a^4 \equiv 0 (\text{mod } 5)$ if $a \equiv 2(\text{mod } 5)$ or $a \equiv 3(\text{mod } 5)$ or if 5 divides a.

Proof. We want to show that if $a \equiv 2(\text{mod } 5)$ or $a \equiv 3(\text{mod } 5)$ or if 5 divides a, then $a^2 + a^4 \equiv 0(\text{mod } 5)$. In other words, we want to show that $a^2 + a^4 = 5k + 0$, where k is an integer. We will do this by considering each of the three cases separately. First let's note some theorems about modular arithmetic that will help us with our proof (Theorem 4, NT-7):

- If $x \equiv m(\text{mod } d)$ and $y \equiv n(\text{mod } d)$, then $x + y \equiv m + n(\text{mod } d)$.
- If $x \equiv m(\text{mod } d)$, then $x^n \equiv m^n(\text{mod } d)$.

<u>Case 1:</u> $a \equiv 2(\text{mod } 5)$
Since $a \equiv 2(\text{mod } 5)$, then $a^2 \equiv 2^2(\text{mod } 5)$ and $a^4 \equiv 2^4(\text{mod } 5)$. $a^2 + a^4 \equiv 2^2 + 2^4(\text{mod } 5) \equiv 20(\text{mod } 5)$. By the definition of mod, we can write $a^2 + a^4 = 5b + 20$ where b is an integer, or $a^2 + a^4 = 5(b + 4) + 0$. Since b is an integer, $b + 4$ must also be an integer. Therefore, if $a \equiv 2(\text{mod } 5)$, then $a^2 + a^4 \equiv 0(\text{mod } 5)$

<u>Case 2:</u> $a \equiv 3(\text{mod } 5)$
Since $a \equiv 3(\text{mod } 5)$, then $a^2 \equiv 3^2(\text{mod } 5)$ and $a^4 \equiv 3^4(\text{mod } 5)$. $a^2 + a^4 \equiv 3^2 + 3^4(\text{mod } 5) \equiv 90(\text{mod } 5)$. By the definition of mod, we can write $a^2 + a^4 = 5c + 90$ where c is an integer, or $a^2 + a^4 = 5(c + 18) + 0$. Since c is an integer, $c + 18$ must also be an integer. Therefore, if $a \equiv 3(\text{mod } 5)$, then $a^2 + a^4 \equiv 0(\text{mod } 5)$

<u>Case 3:</u> 5 divides a
By the definition of divides, $a = 5d$, where d is an integer. So, $a^2 + a^4 = (5d)^2 + (5d)^4 = 25d^2 + 625d^4 = 5(5d^2 + 125d^4) + 0$. Since d is an integer, $5d^2 + 125d^4$ must also be an integer. Therefore, if 5 divides a, then $a^2 + a^4 \equiv 0(\text{mod } 5)$. ■

2. Let x be an integer. Prove that if $x^2 - 6x + 5$ is even then x must be odd.

Proof. Assume for the sake of contradiction that $x^2 - 6x + 5$ is even and x is even. By definition of even, $x = 2c$ where c is an integer. By substitution, $x^2 - 6x + 5 = (2c)^2 - 6(2c) + 5 = 4c^2 - 12c + 5 = 4c^2 - 12c + 4 + 1 = 2(2c^2 - 6c + 2) + 1$. Since $2c^2 - 6c + 2$ is an integer, $x^2 - 6x + 5$ must be odd, which is a contradiction. ■

3. Show that for any posetive number a and b,

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Proof.

$$\frac{a+b}{2} \geq \sqrt{ab} \iff \left(\frac{a+b}{2}\right)^2 \geq ab$$

$$\iff (a+b)^2 = 4ab \iff a^2+b^2+2ab \geq 4ab$$

$$\iff a^2 - 2ab + b^2 \geq 0 \iff (a-b)^2 \geq 0$$

Since square on any number is greater than zero so the $(a-b)^2 \geq 0$ and so we have the inequality. ■

4. If a is an odd integer prove that $a^2 - 1$ is always divisible by 8.

Proof. If a is divided by 4 then the possible set of remainders are $0, 1, 2$ and 3.

Since a is odd so the remainder when divided by 4 cannot be 0 or 2. So if a is an odd integer then the remainder when divided by 4 is 1 or 3.

Now we do case analysis:

Case 1: Let the remainder be 1. So $a = 4k+1$ for some integer k. Thus

$$a^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2+k) + 1$$

So $a^2 - 1 = 8(2k^2+k)$ and so a^2-1 is divisible by 8.

Case 2: Let the remainder be 3. So $a = 4k+3$ for some integer k. Thus

$$a^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 8(2k^2+3k+1) + 1$$

So $a^2 - 1 = 8(2k^2+3k+1)$ and so a^2-1 is divisible by 8.

■

5. Prove that if k and ℓ are posetive integers then $k^2 - \ell^2$ can never be equal to 2.

Proof. If $a^2 - b^2$ has to be 2 then either both a and b has to be even or both have to be odd. If one is even and the other is odd then $a^2 - b^2$ would be odd.

Now we solve case wise depending on whether both are odd or both are even.

Case 1: Both a and b are even.

Then say $a = 2m$ and $b = 2n$ when m and n are posetive integers.

Then $a^2 - b^2 = (2m)^-(2n)^2 = 4m^2 - 4n^2 = 4(m^2 - n^2)$.

Now since $(m^2 - n^2)$ is an integer and 4 times an integer cannot be 2 so $a^2 - b^2$ cannot be 2 in this case.

Case 2: Both a and b are odd.

Then say $a = 2m + 1$ and $b = 2n + 1$ when m and n are posetive integers. Then

$$a^2 - b^2 = (2m+1)^-(2n+1)^2 = (4m^2 + 4m + 1) - (4n^2 + 4n + 1) = 4(m^2 + m - n^2 - n).$$

Now since $(m^2 + m - n^2 - n)$ is an integer and 4 times an integer cannot be 2 so $a^2 - b^2$ cannot be 2 in this case.

$\blacksquare$

6. Prove that there are infinitely many primes of the form $6k + 5$. That is, consider the primes which has a remainder 5 when divided by 6. Prove that there are infinitely many such primes.

Solution.

— *Left as challenge question* —