# Math 255 - Spring 2017
## Homework 4 Solutions

1. Suppose to the contrary that there are $a, b \in \mathbb{Z}$, with $\gcd(a, b) = 1$, such that $\sqrt{p} = \frac{a}{b}$. Squaring both sides, we get that $p = \frac{a^2}{b^2}$ and clearing the denominator we obtain the equation
$$pb^2 = a^2.$$
From this equation we conclude that $p$ divides $a^2$. By definition of a prime, if $p$ divides a product it must divide one of the factors. In this case this allows us to conclude that $p$ divides $a$.

   Let $k \in \mathbb{Z}$ be such that $a = kp$. Then $a^2 = k^2p^2$, and our equation above becomes
$$pb^2 = k^2p^2.$$
We may divide both sides by $p$ to obtain
$$b^2 = pk^2.$$
We now conclude that $p$ divides $b^2$, and arguing as above, $p$ must divide $b$. This, however, contradicts our assumption that $\gcd(a, b) = 1$ (since $p$ divides both $a$ and $b$), and therefore $\sqrt{p}$ is not a rational number.

2. Let $n = 8$ and $a = 3$, $b = 1$. Then $a \not\equiv b \pmod 8$ because $a - b = 3 - 1 = 2$ is not divisible by 8.

   However, we have
$$a^2 = 1 \equiv 1 \pmod 8$$
and
$$b^2 = 9 \equiv 1 \pmod 8 \quad \text{(because 8 divides } 9 - 1 = 8\text{)}.$$
Hence we see that $a^2 \equiv b^2 \pmod 8$ but $a \not\equiv b \pmod 8$.

   Note that the result should not be surprising at all: Even in the usual $\mathbb{Z}$, if $b = -a \neq 0$, we will have $a \neq b$ but $a^2 = b^2$. The same trick works modulo $n$: If $b \equiv -a \pmod n$, then $b^2 \equiv (-a)^2 \equiv a^2 \pmod n$, since $(-1)^2 \equiv 1 \pmod n$ for all $n$. However, what might be surprising is that this is not the only way to solve this problem! Notice here that if $a = 3$ and $b = 1$ then $b \not\equiv -a \pmod 8$ but still $b^2 \equiv a^2 \pmod 8$. At the end of the semester we will carefully consider the equation $x^2 \equiv a \pmod n$, and we will see when there are only two solutions and when there are more solutions, which might not all just be additive inverses of each other.

3. As mentioned in class, almost any five integers satisfying the premise will give a solution to this problem. Here is one example:

   Let $n = 5$, $a = 2$, $b = 7$ (so $a \equiv b \pmod 5$ since $2 - 7 = -5$ is divisible by 5), $i = 6$ and $j = 1$ (so $i \equiv j \pmod 5$ since $6 - 1 = 5$ is divisible by 5).

Then

$$a^i = 2^6 = 64 \equiv 4 \pmod 5 \quad \text{(because } 64-4=60 \text{ is divisible by 5)}$$

and

$$b^j = 7^1 = 7 \equiv 2 \pmod 5 \quad \text{(because } 7-2=5 \text{ is divisible by 5).}$$

Since $4 \not\equiv 2 \pmod 5$ ($4-2=2$ is not divisible by 5), $a^i \not\equiv b^j \pmod 5$.

Fun fact: If $n = 5$, then the correct condition on the exponents is the following: if $a \equiv b \pmod 5$ and $i \equiv j \pmod 4$, then $a^i \equiv b^j \pmod 5$. Indeed if we keep $a = 2$, $b = 7$, $i = 6$ but now we take $j = 2$, so $i \equiv j \pmod 4$, then we have $a^i \equiv 4 \pmod 5$ still but

$$b^j = 7^2 = 49 \equiv 4 \pmod 5.$$

This is another phenomenon which we will study this later this semester: For any $n$, there is a number $\phi(n)$ such that $a \equiv b \pmod n$ and $i \equiv j \pmod{\phi(n)}$ implies $a^i \equiv b^j \pmod{\phi(n)}$. It so happens that $\phi(5) = 4$, and this is why the second example does work.

4. Instead of computing the large sum and then getting the remainder when we divide by 4, instead we will take the remainder, raise them to then 5, and add those up. From what we've seen in class last Friday, the remainder of that number after division by 4 will be the same as the remainder of the big sum since remainders behave well with respect to multiplication and addition.

   We have that

   $$1^5 + 2^4 + 3^5 + \cdots + 99^5 + 100^5 \equiv 1^5 + 2^5 + 3^5 + 0^5 + \cdots + 3^5 + 0^5 \pmod 4,$$

   because remainders "cycle" through $1, 2, 3$ then 0 when going from one integer to the next. Now on the right hand side, we just have the sum $1^5 + 2^5 + 3^5 + 0^5$ repeated 25 times. Therefore

   $$\begin{aligned} 1^5 + 2^4 + 3^5 + \cdots + 99^5 + 100^5 &\equiv 1^5 + 2^5 + 3^5 + 0^5 + \cdots + 3^5 + 0^5 \pmod 4, \\ &\equiv 25(1^5 + 2^5 + 3^5 + 0^5) \pmod 4. \end{aligned}$$

   We have the following:

   $$\begin{gathered} 25 \equiv 1 \pmod 4 \quad \text{(because } 25-1=24 \text{ is divisible by 4)} \\ 1^5 = 1 \equiv 1 \pmod 4 \\ 2^5 = 32 \equiv 0 \pmod 4 \quad \text{(because } 32-0=32 \text{ is divisible by 4)} \\ 3^5 \equiv (-1)^5 = -1 \equiv 3 \pmod 4 \quad \text{(because } 3-(-1)=4 \text{ is divisible by 4)} \\ 0^5 = 0 \equiv 0 \pmod 4. \end{gathered}$$

Therefore we now have

$$\begin{aligned} 1^5 + 2^4 + 3^5 + \cdots + 99^5 + 100^5 &\equiv 25(1^5 + 2^5 + 3^5 + 0^5) \pmod 4 \\ &\equiv 1(1 + 0 + 3 + 0) \pmod 4 \\ &\equiv 4 \pmod 4 \\ &\equiv 0 \pmod 4 \end{aligned}$$

and the remainder is 0 when the sum of the problem is divided by 4.

Note that is is correct to say that the big sum is congruent to 0, 4, 8, $-4$, etc. modulo 4, but the question asks for the *remainder*, which must be a number $r$ such that $0 \leq r < 4$. Therefore the only correct answer is 0.