Math 153
Spring 2019

SOLUTIONS TO EXERCISES FROM `aabUpdate09.153.s19.pdf`

1. (*a*) If p is a prime and $0 < k < p$ explain why the binomial coefficient

$$\binom{p}{k} \quad = \quad \frac{p!}{(k!(p-k)!}$$

is divisible by p. [*Hint:* Look for factors of p in the numerator and denominator.]

SOLUTION.

Since $p!/(p-k)! \ = \ (p-k+1)\cdot ...(p-1)p$ and the binomial coefficient is an integer, we know that $k!$ divides this number with zero remainder. Furthermore, if we write $p!/(p-k)! \ = \ qp$ where q is the product of the first $(k-1)$ factors of the product expression, then q is relatively prime to p because all its prime factors are strictly less than p, and similarly for $k!$. By Unique Factorization this means that $k!$ must divide q with zero remainder and hence the binomial coefficient has the form

$$p \cdot \frac{q}{k!}$$

which means itis divisible by p.■

(*b*) Suppose that a and b are integers such that $a \equiv b \bmod (p)$. Show that $a^p \equiv b^p \bmod (p^2)$. [*Hint:* : Write $b = a + kp$.]

SOLUTION.

The Binomial Theorem implies that

$$b^p \quad = \quad (a+kp)^p \quad = \quad \sum_{r=0}^{p} \binom{p}{r} a^{p-r}\,(kp)^r$$

so we need to show that for each $r \geq 1$ the $r^{\rm th}$ term in the right hand summation is divisible by p^2.

If $1 \leq r < p$ this follows because the binomial coefficient and $(kp)^2$ are each divisible by p and hence their product is divisible by p^2. In the remaining case $r = p$ the summand is $(kp)^p$, and this is divisible by p^2 because $p \geq 2$.■

2. (*a*) Suppose that $n > 1$ is an integer and r is another integer such that $r \not\equiv 0, 1 \bmod (n)$ and $r^2 \equiv r \bmod (n)$. Prove that n is not prime. [*Hint:* Use the fact that if n and r are relatively prime then there is some integer q such that $qr \equiv 1 \bmod (n)$.]

SOLUTION.

Follow the hint. Suppose to the contrary that n is prime. Since $r \not\equiv 0 \bmod (n)$ this means that there is some integer q such that $qr \equiv 1 \bmod (n)$. If we multiply both sides of the congruence in the first sentence in the problem by q, we obtain the congruences

$$1 \ \equiv \ qr \ \equiv \ qr^2 \ \equiv \ 1 \cdot r \quad \bmod (n)$$

which contradicts our assumption that $r \not\equiv 0, 1 \bmod(n)$. The source of the problem is our assumption that n is prime, and therefore we conclude that n cannot be a prime number.■

Simple example. Take $n = 6$ and $r = 3$, so that $9 = 3^2 \equiv 3 \bmod(6)$.

(b) Give an example of integers a and n such that $a^n \not\equiv a \bmod(n)$. Note that by the Little Fermat Theorem n cannot be a prime number.

SOLUTION.

Let's see what happens if $n = 6$. The congruence clearly holds if $a = 0, 1$, so let's try $a = 2$. In this case $2^6 = 64 \equiv 4 \bmod(6)$.■

3. (a) Let $n > 1$ be an integer. Explain why $k^2 \equiv (n-k)^2 \bmod(n)$ for all k.

SOLUTION.

By the Binomial Theorem $(n-k)^2 = n^2 - 2nk + k^2$, which is congruent to k^2 mod n.■

(b) Find all integers a such that $0 \leq a \leq 10$ and $a \equiv b^2 \bmod(11)$ for some integer b. [*Hint:* Part (a) may help reduce the amount of calculation needed.]

SOLUTION.

We need only find the classes of $b^2 \bmod(11)$ where $0 \leq b \leq 10$, and by the first part we actually only need to do this for $0 \leq b \leq 5$ since the latter implies $6 \leq (11-b) \leq 11$. — Clearly the classes of $0^2, 1^2, 2^2, 3^2$ are $0, 1, 4, 9$ mod 11, and similarly we have $5 \equiv 4^2 \bmod(11)$ and $3 \equiv 5^2 \bmod(11)$. Therefore the possibilities for b are $0, 1, 3, 4, 5, 9$ mod 11.■

(c) Find all integers a such that $0 \leq a \leq 12$ and $a \equiv b^2 \bmod(13)$ for some integer b.

SOLUTION.

In this case we need only find the classes of $b^2 \bmod(13)$ where $0 \leq b \leq 6$. — Clearly the classes of $0^2, 1^2, 2^2, 3^2$ are $0, 1, 4, 9$ mod 13, and similarly we have $3 \equiv 4^2 \bmod(11)$, and $12 \equiv 5^2 \bmod(13)$ $10 \equiv 6^2 \bmod(11)$. Therefore the possibilities for b are $0, 1, 3, 4, 9, 10, 12$ mod 13.■

The next two problems involve some numerical issues which arise from the Cubic Formula in Chapter 9 of the course notes.

4. The Cubic Formula shows that one root of the polynomial $x^3 - 3x + 1 = 0$ has the form

$$\sqrt[3]{\cos(2\pi/3) + i\sin(2\pi/3)} \ + \ \sqrt[3]{\cos(2\pi/3) - i\sin(2\pi/3)}\ .$$

Express this as a real number; your answer should have the form $K\cos\theta$ for explicit values of K and θ. [*Hint:* $e^{i\alpha} = \cos\alpha + i\sin\alpha$.]

SOLUTION.

The polar form of a complex number $re^{i\alpha}$ is convenient for taking n^{th} roots. In particular, one cube root of this number is given by $r^{1/3}e^{i\alpha/3}$. Therefore the sum of the two cube roots simplifies to

$$\cos(2\pi/9) + i\sin(2\pi/9) \ + \ \cos(2\pi/9) - i\sin(2\pi/9)$$

which of course is equal to $2\cos(2\pi/9)$.■

5. The Cubic Formula shows that one root of the polynomial $x^3 + x^2 - 2 = 0$ has the form

$$\frac{1}{3}\left(\sqrt[3]{26 + 15\sqrt{3}} \;+\; \sqrt[3]{26 - 15\sqrt{3}} \;-\; 1\right) .$$

Using Bombelli's methods, show that this expression is a positive integer (in fact, an extremely familiar value). The crucial step is to express the expressions under the cube root signs as $a \pm b\sqrt{3}$ for two single digit integers a and b.

SOLUTION.

Follow the hint in the final sentence and try to write $26 + 15\sqrt{3} = \left(a + b\sqrt{3}\right)^3$ for suitable a and b. Expanding the right hand side yields

$$a^3 + 3a^2b\sqrt{3} + 3a(3b^2) + 9b^3\sqrt{3}$$

and if we equate coefficients we obtain the equations $a^3 + 9b^2 = 26$ and $3a^2b + 9b^3 = 15$.

Generally systems of equations like the preceding do not yield much information, but the final sentence helps because it asks for solutions where a and b are single digit integers. Let's start by looking for solutions where both integers are positive. Then the second equation implies that b must be equal to 1, which in turn implies that a must be equal to 2. We should now check that $26 \pm 15\sqrt{3} = \left(2 \pm \sqrt{3}\right)^3$, but the latter are routine exercises.

Finally, if we substitute this into the Cubic Formula expression we see that the latter simplifies to

$$\frac{1}{3}\left((2 + \sqrt{3}) \;+\; (2 - \sqrt{3}) \;-\; 1\right)$$

which in turn simplifies to 1. To check the accuracy of our calculations we should verify that 1 is a root of the original cubic polynomial, but this is very easy to do.∎