

MAS 117

Introduction to Algebra

Solutions 6

February 2007

1 In $\mathbb{Z}_{13}$, we have $3 \times 9 = 5 \times 8 = 1$. [How do you find this? Either by trial and error – run through numbers congruent to 1 mod 13 until you reach a value divisible by 3 or 5 respectively – or use the extended Euclidean algorithm to express $\gcd(3, 13)$ as $3x + 13y$, etc.] Thus

$$\frac{2}{3} + \frac{3}{5} = 2 \cdot 9 + 3 \cdot 8 = 42 = 3$$

in $\mathbb{Z}_{13}$, or more formally $[3]_{13}$.

2 This can be solved by trial and error: compute the squares mod 17 and mod 19 to find all congruent to 2. But we could observe that there are at most two solutions. For suppose that a is a solution, so that $a^2 = 2$ in $\mathbb{Z}_p$. Then if x is any solution, then $0 = x^2 - 2 = x^2 - a^2 = (x + a)(x - a)$, and if the product of two elements of $\mathbb{Z}_p$ is zero, then one factor must be zero; so $x = a$ and $x = -a$ are the two solutions.

So, as $6^2 \equiv_{17} 2$, the solutions in $\mathbb{Z}_{17}$ are ± 6 , or $[6]_{17}$ and $[11]_{17}$.

There are no solutions in $\mathbb{Z}_{19}$. The squares are 1, 4, 5, 6, 7, 9, 11, 16, 17.

3 (a) Using the first definition, take a set of n elements, one of which (called A) is distinguished in some way. There are $\binom{n}{r}$ ways of choosing a subset of size r . Of these, some contain A and others do not. The number containing A is equal to the number of ways of choosing $r - 1$ more elements from the remaining $n - 1$, which is $\binom{n-1}{r-1}$. The number not containing A must be entirely made up from the remaining $n - 1$ elements, so there are $\binom{n-1}{r}$ of them.

Using the second definition,

$$\begin{aligned} \binom{n-1}{r-1} + \binom{n-1}{r} &= \frac{(n-1)!}{(r-1)!(n-r)!} + \frac{(n-1)!}{r!(n-r-1)!} \\ &= \frac{(n-1)!}{r!(n-r)!} (r + (n-r)) \\ &= \frac{n \times (n-1)!}{r!(n-r)!} \end{aligned}$$

$$= \binom{n}{r}.$$

(b) Starting the induction: the result is clearly true for $n = 1$ since $\binom{1}{0} = \binom{1}{1} = 1$. Suppose that

$$(x+y)^{n-1} = \sum_{r=0}^{n-1} \binom{n-1}{r} x^r y^{n-1-r}.$$

To get $(x+y)^n$, we multiply this by $x+y$. How do we get a term $x^r y^{n-r}$ in the product? This comes either by taking the term $x^{r-1} y^{n-r}$ (with coefficient $\binom{n-1}{r-1}$) and multiplying by x , or by taking the term $x^r y^{n-r-1}$ (with coefficient $\binom{n-1}{r}$) and multiplying by y . So the coefficient of $x^r y^{n-r}$ in $(x+y)^n$ is

$$\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r},$$

by part (a).

Here is a different proof, not using induction. Consider

$$(x+y)^n = (x+y)(x+y) \cdots (x+y).$$

On the right, we have n factors $x+y$. In order to get a term $x^r y^{n-r}$, we have to choose x from r of these factors and y from the other $n-r$ and multiply them together. The number of ways of choosing the r factors which contribute x is $\binom{n}{r}$. So the coefficient of $x^r y^{n-r}$ is $\binom{n}{r}$.

(c) For $1 \leq r \leq p-1$, we have

$$\binom{p}{r} = \frac{p!}{r!(p-r)!}.$$

The numerator is the product of all the integers from 1 to p , and so is divisible by p ; but all factors of the denominator are less than p . So, after cancellation, the prime factor p remains.

4 We prove that $n^p \equiv_p n$ by induction on n ; the induction starts when $n = 1$ where it is obviously true.

Suppose that $n^p \equiv_p n$. By the Binomial Theorem,

$$(n+1)^p = n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1.$$

By part (a), the terms in the summation in the middle are all divisible by p ; so

$$(n+1)^p \equiv_p n^p + 1 \equiv_p n + 1,$$

where in the last step we used the induction hypothesis. This completes the induction step.