0.1 Fractions Mod p and Wolstenholme's theorem

1 [GhEw pp.104] (Wolstenholme's Theorem)

PEN A23

Prove that if $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}$ is expressed as a fraction, where $p>3$ is a prime, then p^2 divides the numerator.

2 [Putnam 1996] Let $p>3$ be a prime number and $k=\lfloor\frac{2p}{3}\rfloor$ Prove that $\binom{p}{1}+\binom{p}{2}+\cdots+\binom{p}{k}$ is divisible by p^2

PEN A24

A23. First we will prove some easy elementary facts that will allow us to work with fractions *modp*. This is very useful in some problems but it's not well known. Sometimes, when students are taught congruences they don't think of things such as $k\equiv\frac{1}{2}\pmod p$, because it doesn't seem quite natural. But in fact we will see that this makes pefect sense, as long as we are careful that the denominators are relatively prime to the modulus (it's equivalent to the fact that we cannot divide by zero in usual fractions).

Definition 1: Let b and m be integers such that $gcd(b,m)=1$

$$k\equiv\frac{1}{b}\pmod m\iff bk\equiv 1\pmod m \tag{1}$$

This notation makes perfect sense because k, which is the multplicative inverse of b $modm$ exists,since $gcd(b,m)=1$ and it's trivial to see that k is uniquely determined. Moreover the equivalency between both equations is clear when multypling or dividing by b (it can be done since $gcd(b,m)=1$)

When we see something like $\frac{a}{b}$ $modm$ with $(b,m)=1$ we can think of the fraction like an integer k which satisfies $bk\equiv a\pmod m$

Now we will present the proof of A23

First of all, we can see that that all the denominators are not multiple of p so, as previously showed, we can treat them as integers, so we are left to prove that for $p>3$

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\equiv 0\pmod{p^2} \tag{2}$$

Since $p>3$ is odd, there are an even number of terms in the summation. An useful idea in this kind of problems is to make pairs of numbers in the summation. A natural way of doing this is to sum up the pair of number of the form $\frac{1}{i}$ and $\frac{1}{p-i}$ Then $\frac{1}{i}+\frac{1}{p-i}=\frac{p-i+i}{(p-i)i}=\frac{p}{(p-i)i}$ (I) Since $p>2$

our problem is equivalent to prove that

$$2(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1})\equiv 0\pmod{p^2} \tag{3}$$

Using (I) we have to prove that

$$\sum_{i=1}^{p-1} \frac{p}{(p-i)i} \equiv 0 \pmod{p^2} \tag{4}$$

Now we get the p factor out;the expression we have to prove is:

$$\sum_{i=1}^{p-1} \frac{1}{(p-i)i} \equiv 0 \pmod{p} \tag{5}$$

Now we use that

$$p-i \equiv -i \pmod{p} \Longrightarrow \sum_{i=1}^{p-1} \frac{1}{-i^2} \equiv 0 \pmod{p} \tag{6}$$

Since $p > 3$ we can clearly multiply this expression by -1 (We have added a -2 factor to the original equation). Now we have to show that

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \pmod{p} \tag{7}$$

Now we are going to replace $\frac{1}{i}$ by its inverse *modp* If a number is the same as its inverse then we have

$$i^2 \equiv 1 \pmod{p} \tag{8}$$

So $i \equiv 1 \pmod{p}$ or $i \equiv -1 \pmod{p}$

Now if we consider the numbers $\frac{1}{i}$ with i between 2 and $p-2$ we have an even amount of numbers, each of whom has an inverse in that interval. As a conclusion the equation (6) can be rewritten as:

$$\sum_{i=1}^{p-1} i^2 \equiv 0 \pmod{p} \tag{9}$$

Luckily there is a closed form for calculating the sum of the first n squares, which can be easily proved by straightforward induction.

$$\sum_{i=1}^{p-1} i^2 = \frac{p(p+1)(2p+1)}{6} \equiv 0 \pmod{p} \tag{10}$$

(Since $p > 3$, 6 is relatively prime to p) That finishes the proof of the problem. □

This theorem, and the technique used to solve them,is very useful in lots of problems,for example, Iberoamerican 2005 problem 3 and APMO 2006 problem 3. The reader might be interested in solving this problems without this ideas and find how difficult they are. However, using fractions *modp* and the ideas used to solve A23, they will find that they are not so difficult problems. In addition problem 4 of IMO 2005 was a lot easier if the contestant was used to fractions *modp*. This examples shows that this idea, despite the fact that it is very simple, allows to us to tackle some tough problems. Now we will provide a proof for A24, and in the way we will find an easy generalization for A32 (IMO 1979 problem 1)

A 24. First we state A32 [IMO 1979/1] Let a and b be natural numbers such that

$$\frac{a}{b} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319} \tag{11}$$

Prove that a is divisible by 1979

We will rewrite the statement of A24 as

$$\sum_{i=1}^{k} \frac{(p-1)!p}{(p-i)!i!} \equiv 0 \pmod{p^2} \tag{12}$$

We get rid of the p in the summation and we have to prove that

$$\sum_{i=1}^{k} \frac{(p-1)!}{(p-i)!i!} \equiv 0 \pmod{p} \tag{13}$$

Now we compute

$$\frac{(p-1)!}{(p-i)!} = (p-i+1)(p-i+2)\cdots(p-1) \tag{14}$$

And

$$p - i + j \equiv (-1)(i-j) \pmod{p} \tag{15}$$

Putting (13) and (14) into (12) $\Longrightarrow$

$$\sum_{i=1}^{k} \frac{((-1)^{i-1})(i-1)!}{i!} \equiv 0 \pmod{p} \Longrightarrow \sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} \equiv 0 \pmod{p} \tag{16}$$

Since 1979 is a prime, and in this case $k = 1319$, we find that the statement of A32 is equivalent to showing the generalization provided by (15) Now we will continue our proof. Since $p > 3$, $p = 6l + 1$ or $p = 6l - 1$

Case 1) $p = 6l + 1 \Longrightarrow k = 4l$

$$\sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} = (\sum_{i=1}^{4l} \frac{1}{i}) - 2(\sum_{i=1}^{2l} \frac{1}{2i}) = (\sum_{i=1}^{4l} \frac{1}{i}) - (\sum_{i=1}^{2l} \frac{1}{i}) = (\sum_{i=2l+1}^{4l} \frac{1}{i}) \tag{17}$$

Now, as previosuly done in A23, we will make pair of numbers of the form $\frac{1}{2l+t}$ and $\frac{1}{4l+1-t} \Longrightarrow$

$$\frac{1}{2l+t} + \frac{1}{4l+1-t} = \frac{2l+t+4l+1-t}{(4l+1-t)(2l+t)} = \frac{6l+1}{(4l+1-t)(2l+t)} = \frac{p}{(4l+1-t)(2l+t)} \tag{18}$$

Since the range of t is the numbers between 1 and l, the denominators are relatively prime to p. Moreover, each term of the form $\frac{1}{2l+t}$ has a pair which forms a multiple of p in equation (16), so 16 can be rewritten as

$$\sum_{i=2l+1}^{4l} \frac{1}{i} = (\frac{1}{2l+1} + \frac{1}{4l}) + (\frac{1}{2l+2} + \frac{1}{4l-1}) + \cdots + (\frac{1}{3l} + \frac{1}{3l+1}) \tag{19}$$

Every pair of number in the parenthesis have a sum $\equiv 0 \pmod{p}$ so the whole summation is a multiple of p, finishing the proof.

Case 2) $p = 6l - 1 \Longrightarrow k = 4l - 1$

$$\sum_{i=1}^{k} \frac{(-1)^{i-1}}{i} = (\sum_{i=1}^{4l-1} \frac{1}{i}) - 2(\sum_{i=1}^{2l-1} \frac{1}{2i}) = (\sum_{i=1}^{4l-1} \frac{1}{i}) - (\sum_{i=1}^{2l-1} \frac{1}{i}) = (\sum_{i=2l}^{4l-1} \frac{1}{i}) \tag{20}$$

Again we rewrite this as

$$\sum_{i=2l}^{4l-1} \frac{1}{i} = (\frac{1}{2l} + \frac{1}{4l-1}) + (\frac{1}{2l+1} + \frac{1}{4l-2}) + \cdots + (\frac{1}{3l-1} + \frac{1}{3l}) \tag{21}$$

Each of the pairs between parenthesis is a multiple of p because

$$\frac{1}{2l-1+t} + \frac{1}{4l-t} = \frac{2l-1+t+4l-t}{(2l-1+t)(4l-t)} = \frac{6l-1}{(2l-1+t)(4l-t)} = \frac{p}{(2l-1+t)(4l-t)} \tag{22}$$

This hold for t between 1 and l, and the denominators are clearly relatively prime to p Since all the terms between parenthesis are a multiple of p the whole summation is a multiple of p and the problem is finished. □

References

1 *PEN Problem A23*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150391

2 *PEN Problem A24*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150392

3 *PEN Problem A32*, http://www.mathlinks.ro/Forum/viewtopic.php?t=150400

4 *Problems suggested* http://www.mathlinks.ro/Forum/resources.php