NOTES

Edited by **Jimmie D. Lawson**

A Simple Congruence modulo p

Winfried Kohnen

Congruences for prime numbers p have always been of great interest. Examples include Fermat's Little Theorem ($n^p \equiv n \pmod p$) or Wilson's theorem ($(p-1)! \equiv -1 \pmod p$). In the following we consider the congruence relation modulo p extended to the ring of rational numbers with denominators not divisible by p. For such fractions $m/n \equiv r/s \pmod p$ if and only if $ms \equiv nr \pmod p$, and the residue class of m/n is the residue class of m times the inverse of the residue class of n in $\mathbf{Z}_\mathbf{p}$.

The purpose of this note is to state and prove the following result.

Theorem. *Let p be an odd prime. Then*

$$\sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv \sum_{k=1}^{(p-1)/2} \frac{(-1)^{k-1}}{k} \pmod p. \tag{1}$$

Proof: First note the identity

$$\sum_{k=1}^{N} \frac{1}{k}(1-X)^k = \sum_{k=1}^{N} \frac{(-1)^k}{k}\binom{N}{k}(X^k - 1) \quad (N \in \mathbf{N}, x \in \mathbf{R}). \tag{2}$$

Indeed, the derivative of the left-hand side of (2) is

$$-\sum_{k=1}^{N}(1-X)^{k-1} = -\frac{1-(1-X)^N}{1-(1-X)} = \frac{(1-X)^N - 1}{X},$$

while the derivative of the right-hand side is

$$\sum_{k=1}^{N}(-1)^k\binom{N}{k}X^{k-1}.$$

Hence the derivative of both sides are equal. Also (2) is true for $X = 1$.

In (2) we set $N = p - 1$ and $X = -1$. From $p - k \equiv -k \pmod p$, we deduce

$$\binom{p-1}{k} = \frac{(p-1)\cdots(p-k)}{k!} \equiv (-1)^k \pmod p$$

and

$$\sum_{k=1}^{p-1}\frac{1}{k} = \sum_{k=1}^{p-1}\frac{1}{p-k} \equiv -\sum_{k=1}^{p-1}\frac{1}{k} \equiv 0 \pmod p,$$

and thus equation (2) simplifies to

$$\sum_{k=1}^{p-1} \frac{2^k}{k} \equiv \sum_{k=1}^{p-1} \frac{(-1)^k}{k} \pmod{p}. \tag{3}$$

In the sum on the left we replace k by $p - k \equiv -k \pmod{p}$ and use Fermat's Little Theorem to obtain

$$\sum_{k=1}^{p-1} \frac{2^k}{k} \equiv -2^p \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \equiv -2 \sum_{k=1}^{p-1} \frac{1}{k \cdot 2^k} \pmod{p}.$$

The sum on the right of (3) we rewrite as

$$\sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} + \sum_{k=1}^{(p-1)/2} \frac{(-1)^{p-k}}{p-k} \equiv 2 \sum_{k=1}^{(p-1)/2} \frac{(-1)^k}{k} \pmod{p}.$$

This proves (1).

In the literature, congruences of a type similar to (1) can be found; however, in general they are of a much deeper nature. For example, in [1] with the help of properties of the Pell sequence $((1+\sqrt{2})^n)_{n \in N}$ it is shown that

$$\sum_{k=1}^{(p-1)/2} \frac{1}{k \cdot 2^k} \equiv \sum_{k=1}^{[3p/4]} \frac{(-1)^{k-1}}{k} \pmod{p}. \tag{4}$$

It seems unlikely that (4) can be proved with the simple approach we have used here.

REFERENCE

1. Zhi-Wei Sun, A congruence for primes, *Proc. Amer. Math. Soc.* 123 (1995), 1341–1346.

Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg, Germany
winfried@mathi.uni-heidelberg.de

A Geometrical Method for Finding an Explicit Formula for the Greatest Common Divisor

Marcelo Polezzi

This note presents an explicit formula for the greatest common divisor (g.c.d.) of two integers derived using a simple geometrical argument.

In [1], chapter 3, an expression was deduced, from which one can easily obtain a formula for the g.c.d. as a particular case. However, the derivation of that expression is very tiring and lengthy.