A Geometrical Method for Finding an Explicit Formula for the Greatest Common Divisor
Author(s): Marcelo Polezzi
Source: *The American Mathematical Monthly*, Vol. 104, No. 5 (May, 1997), pp. 445-446
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2974739
Accessed: 24/03/2010 21:25

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/page/info/about/policies/terms.jsp. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/action/showPublisher?publisherCode=maa.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

http://www.jstor.org

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

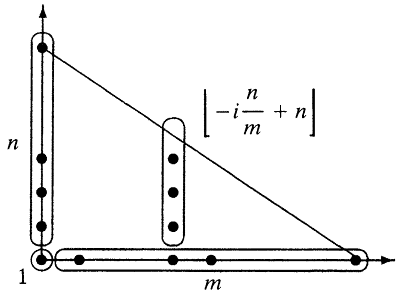
Marcelo Polezzi

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.

Here is the result to be proved:

Theorem. *Let m and n be positive integers. Then g.c.d.$(m, n) = 2\sum_{i=1}^{m-1}\left\lfloor i\frac{n}{m}\right\rfloor + (m + n) - mn$, where $\lfloor x\rfloor$ is the greatest integer less than or equal to x.*



Proof: Consider the triangle $M = \left\{(x, y) \in \mathbb{R}^2 | x \geq 0; y \geq 0; y \leq -\frac{n}{m}x + n\right\}$. We have

$$\#(M \cap \mathbb{Z}^2) = \sum_{i=1}^{m-1}\left\lfloor -i\frac{n}{m} + n\right\rfloor + (m + n + 1)$$
$$= \sum_{i=1}^{m-1}\left\lfloor (m - i)\frac{n}{m}\right\rfloor + (m + n + 1) = \sum_{i=1}^{m-1}\left\lfloor i\frac{n}{m}\right\rfloor + (m + n + 1). \quad (1)$$

On the other hand, by considering the triangle as half of a rectangle, we obtain

$$\#(M \cap \mathbb{Z}^2) = \frac{(m + 1)(n + 1) + (d + 1)}{2} \quad (2)$$

where $d = g.c.d.(m, n)$, since the number of lattice points on the hypotenuse is equal to $(d + 1)$. In fact, let $y_i = -(n/m)x_i + n$. The set of integers x_i between 0 and m such that y_i is an integer is

$$\left\{0, \frac{m}{d}, 2\frac{m}{d}, \ldots, (d - 1)\frac{m}{d}, m\right\}.$$

Hence, equating (1) and (2), we have

$$\sum_{i=1}^{m-1}\left\lfloor i\frac{n}{m}\right\rfloor + (m + n + 1) = \frac{(m + 1)(n + 1) + (d + 1)}{2}.$$

Therefore, $d = 2\sum_{i=1}^{m-1}\left\lfloor i\frac{n}{m}\right\rfloor + (m + n) - mn$.

Remark. The formula clearly holds for $n = 0$.

REFERENCE

1. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics—A Foundation for Computer Science*, Addison-Wesley Publishing Company, 1994.

Departamento de Matemática
Instituto de Biociências, Letras e Ciências Exatas
Universidade Estadual Paulista
São José do Rio Preto-S.P-CP 136
Brazil