Wilson's theorem

Monika rathore

February 2018

1 Introduction

1.1 Proofs

Suppose first that p is composite. Then p has a factor $d > 1$ that is less than or equal to $p - 1$. Then d divides $(p-1)!$, so d does not divide $(p-1)! + 1$. Therefore p does not divide $(p-1)! + 1$.

Two proofs of the converse are provided: an elementary one that rests close to basic principles of modular arithmetic, and an elegant method that relies on more powerful algebraic tools.

1.2 Elementry proof

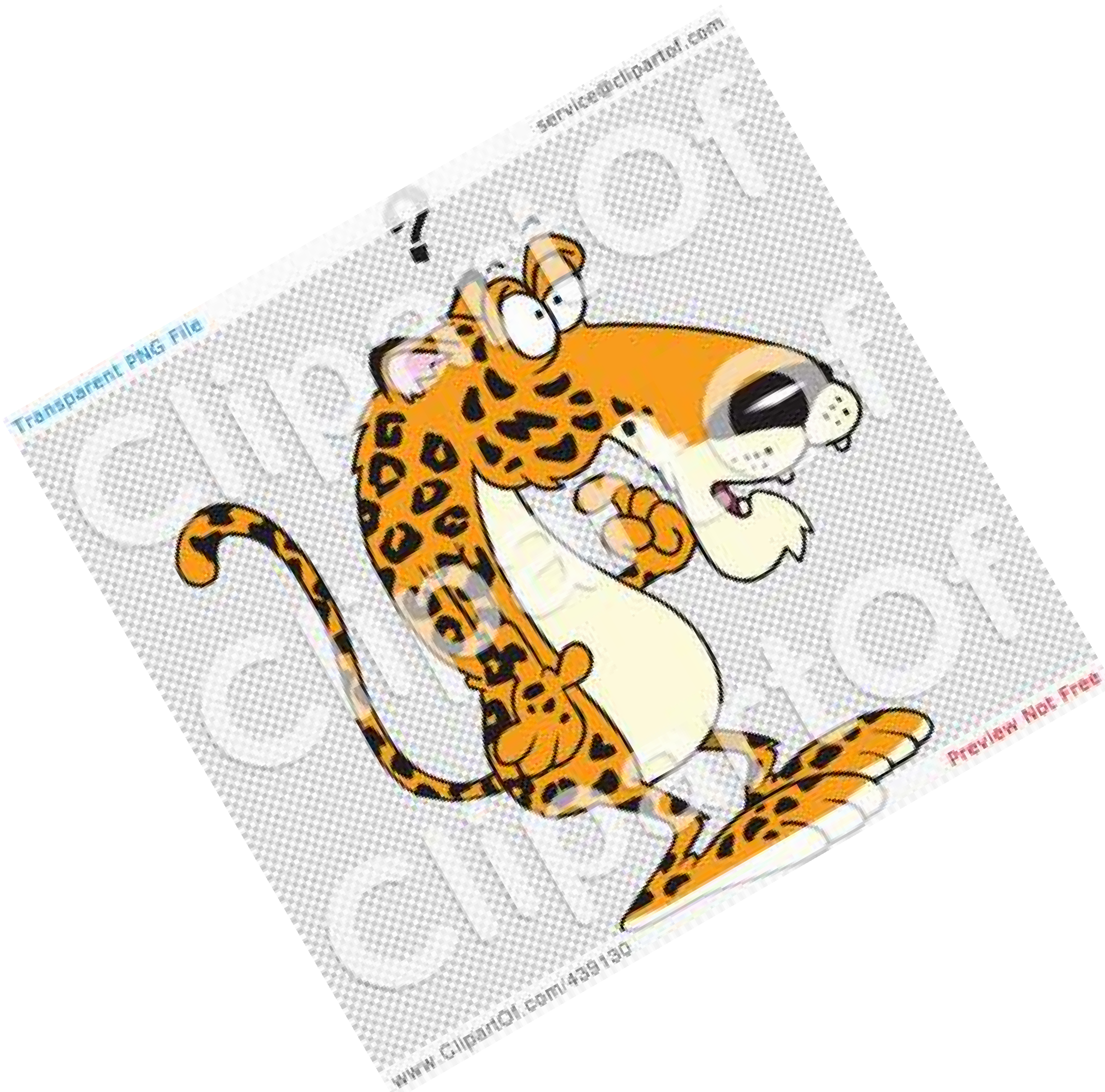
Suppose p is a prime. Then each of the integers $1, ..., p-1$ has an inverse modulo p. (Indeed, if one such integer a does not have an inverse, then for some distinct b and c modulo p, $ab \equiv ac \pmod{p}$, so that $a(b-c)$ is a multiple of p, when p does not divide a or $b-c$—a contradiction.) This inverse is unique, and each number is the inverse of its inverse.
If one integer a is its own inverse, then

$$0 \equiv a^2 - 1 \equiv (a-1)(a+1) \pmod{p}, \tag{1}$$

so that $a \equiv 1$ or $a \equiv p - 1$. Thus we can partition the set $\{2, \ldots, p-2\}$ into pairs $\{a, b\}$ such that $ab \equiv 1 \pmod{p}$. It follows that $(p-1)$ is the product of these pairs times $1 \cdot (-1)$. Since the product of each pair is conguent to 1 modulo p, we have

$$(p-1)! \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}, \tag{2}$$

Figure 1: Confused



1.3 Algebric Proof

Let p be a prime. Consider the field of integers modulo p.
By Fermat's Little Theorem, every nonzero element of this field is a root of the

polynomial

$$P(x) = x^{p-1} - 1 \tag{3}$$

. Since this field has only $p-1$ nonzero elements, it follows that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1} (x - r). \tag{4}$$

Now, either $p = 2$, in which case $a \equiv -a \pmod 2$ for any integer a, or $p-1$ is even. In either case, $(-1)^{p-1} \equiv 1 \pmod p$, so that

$$x^{p-1} - 1 = \prod_{r=1}^{p-1} (x - r) = \prod_{r=1}^{p-1} (-x + r). \tag{5}$$