Dr. Z.'s Number Theory Lecture 13 Handout: Wilson's Theorem and Fermat's little theorem

By Doron Zeilberger

Wilson's Theorem: If $n > 1$ is a natural number, $(n-1)! \equiv -1 \pmod{n}$ iff n is a prime.

Problem 13.1: Check empirically Wilson's theorem for (i) $n = 6$ and (ii) $n = 7$.

Solution of 13.1:

(i) $5! \pmod{6} = 120 \equiv 0 \pmod{6}$, and this is **not** $-1 \equiv \pmod{6}$.

(ii) $6! \pmod{7} = 720 \pmod{7} = 721 - 1 \pmod{7} \equiv 7 \cdot 103 - 1 \pmod{7} \equiv -1 \pmod{7}$.

Proof of Wilson's theorem for n composite: If n is composite, it is divisible by some prime q, $2 \leq q \leq n-2$. So $(n-1)!$ is divisible by q. But if $(n-1)! \equiv -1 \pmod{n}$ then $(n-1)! \equiv -1 \pmod{q}$, contradiction.

Proof for n prime: We have to show that if p is prime then $(p-1)! \equiv -1 \pmod{p}$.

For $p = 2$: $1! \equiv -1 \pmod{2}$.

If $p > 2$, then for any a, $1 \leq a \leq p-1$, there exists a b, $1 \leq b \leq p-1$, such that $ab \equiv 1 \pmod{p}$ (recall that it called the multiplicative inverse, denoted by $a^{-1} \pmod{p}$). If $a \equiv a^{-1} \pmod{p}$ then $a^2 - 1 \equiv 0 \pmod{p}$, so $(a-1)(a+1) \equiv 0 \pmod{p}$ that has two roots modulo p: $a \equiv 1 \pmod{p}$, and $a \equiv -1 \pmod{p}$). So, we can arrange all the integers $1, 2, \ldots, p-1$, except for 1 and $p-1$, into **pairs** $\{a, b\}$, such that $ab \equiv 1 \pmod{p}$ except for 1 and $p-1$ whose product is $-1 \pmod{p}$. $\square$

Problem 13.2: Illustrate the proof of Wilson's theorem for $p = 13$.

Solution to 13.2:

$$2^{-1} \pmod{13} = 7 \quad , \quad 3^{-1} \pmod{13} = 9 \quad , \quad 4^{-1} \pmod{13} = 10 \quad ,$$
$$5^{-1} \pmod{13} = 8 \quad , \quad 6^{-1} \pmod{13} = 11 \quad .$$

So

$$12! = (1 \cdot 12)(2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv (-1)(1)(1)(1)(1)(1) \pmod{13} \equiv -1 \pmod{13} \quad .$$

Fermat's little theorem:

If p is a prime number, then for any integer a, $(a^p - a)/p$ is always an integer. In other words

$$a^p \equiv a \pmod{p} \quad .$$

Problem 13.3: Check, empirically, Fermat's little theorem for $p = 7$.

Solution to 13.3:

$(1^7 - 1)/7 = 1$

$(2^7 - 2)/7 = 126/7 = 18$

$$3 \pmod 7 = 3 \quad , \quad 3^2 \pmod 7 = 2 \quad , \quad 3^4 \pmod 7 = 2^2 = 4 \pmod 7$$

So

$$3^7 \pmod 7 = 3^4 \cdot 3^2 \cdot 3 \pmod 7 = 4 \cdot 2 \cdot 3 = 24 \equiv 3 \pmod 7 \quad .$$

$$4 \pmod 7 = 4 \quad , \quad 4^2 \pmod 7 = 2 \quad , \quad 4^4 \pmod 7 = 2^2 = 4 \pmod 7 \quad .$$

So

$$4^7 \pmod 7 = 4^4 \cdot 4^2 \cdot 4 \pmod 7 = 4 \cdot 2 \cdot 4 = 32 \equiv 4 \pmod 7 \quad .$$

$$5^7 \pmod 7 = (-2)^7 \pmod 7 = -2^7 \pmod 7 = -2 \pmod 7 = 5 \pmod 7$$

$$6^7 \pmod 7 = (-1)^7 \pmod 7 = -1^7 \pmod 7 = -1 \pmod 7 = 6 \pmod 7 \quad .$$

First Proof of Fermat's little theorem:: Recall the binomial theorem

$$(x+1)^n = x^n + \frac{n}{1}x^{n-1} + \frac{n(n-1)}{1 \cdot 2}x^{n-2} + \ldots + \frac{n(n-1)\cdots(n-k+1)}{1 \cdots k}x^{n-k} + \ldots + 1 \quad .$$

When p is prime:

$$(x+1)^p = x^p + \frac{p}{1}x^{p-1} + \frac{p(p-1)}{1 \cdot 2}x^{n-2} + \ldots + \frac{p(p-1)\cdots(p-k+1)}{1 \cdots k}x^{p-k} + \ldots + 1 \quad .$$

But $\frac{p(p-1)\cdots(p-k+1)}{1\cdots k}$ is always divisible by p, for $k = 1.., p-1$ (why?), so modulo p

$$(x+1)^p \equiv x^p + 1 \pmod p \quad .$$

Starting with the obvious $0^p \equiv 0 \pmod p$, we have $1^p \equiv 1 \pmod p$, $2^p \equiv 2 \pmod p$, and *by induction* on a, $a^p \equiv \pmod p$, for **all** a from 0 to $p-1$, and hence for all a whatsoever. $\square$

Second Proof of Fermat's little theorem:: If $p = 2$ it is trivial (why?). If $a = 0$ it is also trivial.

If $p > 2$, and $1 \leq a \leq p-1$, then $a, 2a, 3a, \ldots, (p-1)a$, modulo p, are **distinct** (since if $ai \equiv aj \pmod{p}$ then $a(i-j)$ is divisible by p, hence $i-j$ is divisible by p hence $i \equiv j \pmod{p}$ (and $i = j$ since we assume that they are between 0 and $p-1$).

So the product of all the members of $\{1, 2, \ldots, p-1\}$ modulo p, (alias $(p-1)! \pmod{p}$) is the same, modulo p, as the product of

$$a \quad , \quad 2a, \quad \ldots \quad , \quad a(p-1) \quad ,$$

is the same as

$$(a)(2a)(3a) \cdot ((p-1)a) = a^{p-1}(p-1)! \pmod{p} \quad .$$

So

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Since $(p-1)!$ is **not** 0 modoluo p, we can divide by it, and get that for $0 < a \leq p-1$

$$a^{p-1} \equiv 1 \pmod{p} \quad .$$

Multiplying both sides by a proves it. □

Problem 13.4: Illustrate the Second proof of Fermat's little theorem with $p = 5$ and $a = 3$.

Solution to 13.4:

$$3 \cdot 1 \pmod{5} = 3 \quad , \quad 3 \cdot 2 \pmod{5} = 1 \quad , \quad 3 \cdot 3 \pmod{5} = 4 \quad , \quad 3 \cdot 4 \pmod{5} = 2 \quad .$$

Since $[3, 1, 4, 2]$ is a permutation of $[1, 2, 3, 4]$, we have:

$$(3 \cdot 1)(3 \cdot 2)(3 \cdot 3)(3 \cdot 4) \equiv (1)(2)(3)(4) \equiv$$

So

$$3^4 \cdot 4! \equiv 1 \cdot 4! \pmod{5} \quad .$$

Dividing by $4! = 24$ (**not** 0 modulo 5), we get

$$3^4 \equiv 1 \pmod{5} \quad .$$

Multiplying both sides by 3, we get

$$3^5 \equiv 3 \pmod{5} \quad .$$

Third Proof of Fermat's little theorem:: If p is a prime then $(a^p - a)/p + a$ is the number of necklaces (without a clasp) with p beads of a different colors. (See very end of page 10 and very beginning of page 11 of
`http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimPDF/enu.pdf`). Since it counts a finite set, it must be an integer.

Problem 13.5: How many necklaces of length 3 are there with red and green beads? Write them all down.

Solution to 13.5: Here $a = 2$ and $p = 3$ so the number of necklaces is $(2^3 - 2)/3 + 2 = 2 + 2 = 4$.

The two necklaces with the same colors are

$$GGG \quad , \quad RRR$$

Let's first list all 2^3 **linear necklaces** for length 3 with colors $\{G, R\}$

$$GGG, GGR, GRG, GRR, RGG, RGR, RRG, RRR \quad .$$

The first and last are **monochromatic**, and the remaining one fall naturally into **equivalence classes** by rotation.

$$\{GGR, GRG, RGG\} \quad ,$$

and

$$\{GRR, RRG, RGR\} \quad .$$

Solution to 13.5: There are four necklaces:

GGG,

RRR,

GGR (alias GRG, alias RGG), and

GRR (alias RRG, alias RGR).