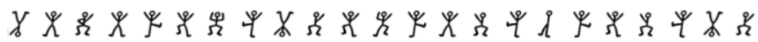
MATH 1025: Introduction to Cryptography

Bonus 4



generosity of reciprocity

The product of even numbers modulo p can be written in two different ways[1]

$$2\cdot 4\cdot 6\cdot \ldots \cdot (p-1) \equiv 2\cdot 4\cdot \ldots \cdot 2\cdot \left\lfloor \frac{p-1}{4} \right\rfloor \cdot \left(-2\cdot \left\lfloor \frac{p-1}{4} \right\rfloor -1\right)\cdot \left(-2\cdot \left\lfloor \frac{p-1}{4} \right\rfloor -1+3\right)\cdot \left(-2\cdot \left\lfloor \frac{p-1}{4} \right\rfloor -1+5\right)\cdot \ldots \cdot (-1) \pmod p \tag{0.1}$$

Example. Let's take $p = 11$, then

$$2\cdot 4\cdot 6\cdot 8\cdot 10 \equiv 2\cdot 4\cdot (-5)\cdot (-3)\cdot (-1) \pmod{11}.$$

Problem.

(a) [2 **pts**] Derive from the congruence (0.1) above the congruence

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\left\lceil \frac{p-1}{4} \right\rceil} \left(\frac{p-1}{2}\right)! \pmod p, \tag{0.2}$$

where $\lceil x \rceil$ is the least integer greater than or equal to x.

(b) [2 **pts**] Using Euler's property, conclude that the Legendre symbol

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8 \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

[1]To obtain the r.h.s., substitute every number a in the l.h.s., greater than $(p-1)/2$, by $p-a$.