HW04 CoderBak

I. Celebrate and Remember Textiles

$$\left.\begin{aligned} n &\equiv 4 \pmod 7 \\ n &\equiv 2 \pmod 4 \\ n &\equiv 2 \pmod 5 \end{aligned}\right\} \longrightarrow n = 35k - 3$$

$$35k - 3 \equiv 2 \pmod 4 \quad \Rightarrow \quad k \equiv -1 \pmod 4$$

$$35 \times 3 - 3 = 102$$

II. Euler's Totient Theorem

(a). We claim that $(am_i, n) = 1$

Also $am_i \not\equiv am_j \pmod n$. #

(b) $\prod am_i = a^{\varphi(n)} \prod m_i \equiv \prod m_i \pmod n$.

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

III. Sparsity of Primes

Prove: $\forall k$, there exists k consecutive integers, none of them $= p^2$

Construct n, $n+1 \sim n+k \neq p^2$ select $p_i \cdot q_i > k$. $p_i \neq p_j$ $q_i \neq q_j$ $p_i \neq q_j$

$$\left.\begin{aligned} n+1 &\equiv 0 \pmod{p_1 q_1} \\ n+2 &\equiv 0 \pmod{p_2 q_2} \\ &\vdots \\ n+k &\equiv 0 \pmod{p_k q_k}. \end{aligned}\right. \quad \xRightarrow{CRT} n.$$

IV. RSA Practice.

(a) $N = 55 \qquad (p-1)(q-1) = 40$

$9 \cdot d \equiv 1 \pmod{40} \qquad d = 9$

(b) $4^9 \pmod{55} \equiv 14$

(c) $14^9 \equiv 4 \pmod{55}$

V. Tweaking RSA

(a) $D(E(x)) = x^{ed} \equiv x \pmod{N}$.

$\Rightarrow \quad ed \equiv 1 \pmod{p-1}$

select e which satisfies $(e, p-1) = 1$

then choose $d \equiv e^{-1} \pmod{p-1}$

(b) $d \equiv e^{-1} \pmod{p-1}$

(c) $N = pqr \qquad \varphi(N) = (p-1)(q-1)(r-1)$

$ed \equiv 1 \pmod{\varphi(N) = (p-1)(q-1)(r-1)}$.

choose $d \equiv e^{-1} \pmod{(p-1)(q-1)(r-1)}$.