Next exercise and lecture is on 21. 6. 2019

Lecture Hall of the exam: Audimax

Tutorial 8

P3/: CRT, m_i pairwise relatively prime,

$x \equiv a_i \pmod{m_i} \quad \forall i = 1, \dots, r$

$M = \prod_{i=1}^{r} m_i \qquad x = \sum_{i=1}^{r} a_i M_i y_i \pmod{M} \qquad (1)$

$M_i = M/m_i, \; y_i = M_i^{-1} \pmod{m_i}$ for $i = 1, \dots, r$

a) (1) is a solution

Let $i \neq j$: $m_j \mid M_i \iff M_i \equiv 0 \pmod{m_j} \qquad (2)$

$\Rightarrow y_i \cdot M_i \equiv 1 \pmod{m_i} \qquad (3)$

Note: We know $\gcd(M_j, m_j) = 1$ because $(m_i)_{i=1,\dots,r}$ are pairwise relatively prime. $\Rightarrow \exists\, y_i \equiv M_i^{-1} \pmod{m_i}$

$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M \overset{(2),(3)}{\equiv} a_j \pmod{m_j}$

b) (1) is unique modulo M

Assume that two different solutions y, z exist.

$y \equiv a_i \pmod{m_i} \wedge z \equiv a_i \pmod{m_i} \quad \forall i = 1, \dots, r$

$\Rightarrow 0 \equiv (y - z) \bmod m_i \quad \forall i = 1, \dots, r$

$\Rightarrow m_i \mid y - z \quad \forall i = 1, \dots, r$

$\Rightarrow M \mid y - z$ as $m_1, \dots, m_r$ are pairwise for $i = 1, \dots, r$

$\Rightarrow y \equiv z \pmod{M}$ ↯

P2| Pollards $p-1$ factoring alg.

a) Just calculate $a^{k!}$ for $k = 1, 2, 3, 4, \dots$ until you find a non-trivial factor by calculating $\gcd(a^{k!} - 1 \bmod n, n)$.

b) When $n = 1403$, $a = 2$, the process of the pollards $p-1$ fact. alg is

	$\gcd(b_i - 1, n)$
$b_1 = a^1 \bmod 1403 = 2$	$d_1 = \gcd(1, 1403) = 1$
$b_2 = b_1^2 \bmod 1403 = 4$	$d_2 = \gcd(3, 1403) = 1$
$b_3 = b_2^3 \bmod 1403 = 64$	$d_3 = \gcd(63, 1403) = 1$
$b_4 = b_3^4 \bmod 1403 = 142$	$d_4 = \gcd(141, 1403) = 1$
$b_5 = b_4^5 \bmod 1403 = 794$	$d_5 = \gcd(793, 1403) = 61 = p$

Therefore, 61 is a non-trivial factor of $1403 = 23 \cdot 61$.
$B = 5$ is sufficient as $p - 1 = 60 = 2^2 \cdot 3 \cdot 5$.
$q = 23$; $q - 1 = 22 = 2 \cdot 11$. To find $q = 23$ with that method you have to take $B = 11$

c) When $n = 25547$, $a = 2$

$b_1 = a^1 \bmod n = 2$ $\quad d_1 = \gcd(1, n) = 1$
$b_2 = b_1^2 \bmod n = 4$ $\quad d_2 = \gcd(3, n) = 1$
$b_3 = b_2^3 \bmod n = 64$ $\quad d_3 = \gcd(63, n) = 1$
$b_4 = b_3^4 \bmod n = 18384$ $\quad d_4 = \gcd(18383, n) = 1$
$b_5 = b_4^5 \bmod n = 23616$ $\quad d_5 = \gcd(23615, n) = 1$
$b_6 = b_5^6 \bmod n = 18620$ $\quad d_6 = \gcd(18619, n) = 433 = p$

Therefore, 433 is a non-trivial factor of $n = 25547 = 433 \cdot 59$.
$B = 6$ is sufficient as $p - 1 = 432 = 2^4 \cdot 3^3$. These are factors within $6!$ but not $5!$ Note that $q - 1 = 58 = 2 \cdot 29$.

P1) Wilson's primality criterion

$n \in \mathbb{N}$ is prime $\Leftrightarrow$ $(n-1)! \equiv (-1) \pmod{n}$

a) Let $n \in \mathbb{N}$ be prime $\Rightarrow$ $\mathbb{Z}_n^* = \{1, \dots, n-1\}$ $\Rightarrow$ all elements have inverses

Moreover, there are two self-inverse elements, namely $1, n-1$.

$\Rightarrow (n-1)! = (n-1)(n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1 \equiv (n-1) \equiv -1 \pmod{n}$

because for all numbers $(n-2), \dots, 3, 2$ there is a unique pair which multiply to one.

b) $28! \equiv -1 \pmod{29}$

c) This criterion is computationally inefficient.