Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

Imdad ullah Khan

Pseudoprimes

Theorem (Ancient Chinese)

Let n be a prime, then $2^{n-1} \equiv_n 1$

Some thought that the converse was also true!

The converse is not true!

$2^{340} \equiv_{341} 1$, but $341 = 31 \cdot 11$

Composites having this property are called pseudoprimes

Fermat's Little Theorem

Theorem (Ancient Chinese)

Let n be a prime, then $2^{n-1} \equiv_n 1$

Theorem (Fermat's Little Theorem)

Let p be a prime, then

- *If $p \nmid a$, then $a^{p-1} \equiv_p 1$*
- *$a^p \equiv_p a$, for every integer a*

Please read your book for Carmichael numbers

Fermat's Little Theorem

Fermat's Little Theorem: Let p be a prime, If $p \nmid a$, then $a^{p-1} \equiv_p 1$

$p = 11$

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Fermat's Little Theorem

Fermat's Little Theorem: Let p be a prime, If $p \nmid a$, then $a^{p-1} \equiv_p 1$

- $p = 11$, $a^{10} = 1$ for all a ▷ [FLT]
- For some a's the exponent gets to 1 before $10 = p - 1$
- Patterns are of lengths that divides 10
- The values a for which all numbers $1 \leq k \leq 10$ appear are called **generators**

Fermat's Little Theorem: Modular Exponentiation

Given int b and ints $n, p \geq 1$, find $b^n \% p$

When modulus is prime, we use FLT to speed up

Find $22^{61} \% 29$

$$22^{61} = 22^{28+28+5} = 22^{28} \cdot 22^{28} \cdot 22^5 = 1 \cdot 1 \cdot 22^5$$

$b^k \% p$ repeats after k reaches $p-1$, so we use

$$b^n \% p = b^{n\%(p-1)} \% p$$

$$22^{61} \% 29 = 22^{61\%28} \% 29 = 22^5 \% 29$$

Fermat's Little Theorem: Modular Exponentiation

$7^{1027} =$

$$
\begin{aligned}
&823544544599327001495546228471606925197566190230622324273960155843749995838247324299808795643737413143459304292037082481398609160820269503301672056029937808578799506374779881698816017119148232704767843317\\
&101102037987772914665213147759018383011564881827311366784706944723048938602116196081664568260010752326060139580331874451190409068034895183321084488463006318582294519193149813795294091072551244801135441743\\
&892785357786574716992541099898150642976554895446350835310499206218444525020034477269414034632300034083364138440845589764562201813493097084222261478784658315332759819862542474620719868157255248265656303202463264976263071006154023466326481984207474225925621916886286895666\\
&771018900540189145255315008975485853411103020176506954639769581265473398166553688960532898916604479386823189147143847468731095247747255673218518774201587365815180289036963117776230459395437321851877420158736581518028903696311777623045939543
\end{aligned}
\quad \% 13 = 6
$$

$$7^{1027} \% 13 = 7^{1027\%12} \% 13 = 7^7 \% 13 = 823543 \% 13 = 6$$