Introduction to Cryptology

Lecture-04
Mathematical Background: Prime Numbers

22.03.2023, v42

Mathematical Background
In Discrete Mathematics, Number Theory

Outlines

Prime Numbers
Primes are necessary to generate finite fields (GF)

Prime numbers like : 2, 3, 5, 7, …..13 ,17 ,19 …..
A prime only divisible by 1 or itself

How many primes do exist between *1* and *n*?
The number of such primes $\pi(n)$ is found to be approximated by:

(Tchebycheff Theorem)
(First indicated by Gauss without proof)

$$\lim_{n\to\infty} \pi(n) = \frac{n}{\ln(n)}$$

Where; ***ln*** **=*log*$_e$ is the** natural logarithm, *e* = ∑ *1/n!* *(for n=1 to ∞) = 2.718..* ***(Euler's number)***

Or $e = \lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x = 2.718281828459\ldots$

Example: The probability that a randomly picked up integer r is a prime number for **1 ≤ r ≤ n= 10^{100} is:**

$$P_r(r = \text{prime}) = \frac{\pi(n)}{n} \approx \frac{1}{\ln(n)} \approx \frac{1}{230} \quad (n = 10^{100})$$

Sample prime numbers

To get a provably prime p, needs exhaustive factorization of p : *Worst case complexity ≈O(√ p)*

List of Primes up to 4483

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73
79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181
191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293	307
311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541	547	557	563	569	571
577	587	593	599	601	607	613	617	619	631	641	643	647	653	659	661	673	677	683	691	701
709	719	727	733	739	743	751	757	761	769	773	787	797	809	811	821	823	827	829	839	853
857	859	863	877	881	883	887	907	911	919	929	937	941	947	953	967	971	977	983	991	997
1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117	1123	1129
1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453
1459	1471	1481	1483	1487	1489	1493	1499	1511	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601
1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753
1759	1777	1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931
1933	1949	1951	1973	1979	1987	1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087
2089	2099	2111	2113	2129	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267
2269	2273	2281	2287	2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399
2411	2417	2423	2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557	2579	2591	2593
2609	2617	2621	2633	2647	2657	2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731
2741	2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079	3083
3089	3109	3119	3121	3137	3163	3167	3169	3181	3187	3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271
3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359	3361	3371	3373	3389	3391	3407	3413	3433	3449	3457
3461	3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539	3541	3547	3557	3559	3571	3581	3583	3593	3607
3613	3617	3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701	3709	3719	3727	3733	3739	3761	3767	3769
3779	3793	3797	3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889	3907	3911	3917	3919	3923	3929	3931
3943	3947	3967	3989	4001	4003	4007	4013	4019	4021	4027	4049	4051	4057	4073	4079	4091	4093	4099	4111	4127
4129	4133	4139	4153	4157	4159	4177	4201	4211	4217	4219	4229	4231	4241	4243	4253	4259	4261	4271	4273	4283
4289	4297	4327	4337	4339	4349	4357	4363	4373	4391	4397	4409	4421	4423	4441	4447	4451	4457	4463	4481	4483

How to Find Probably-Primes ?

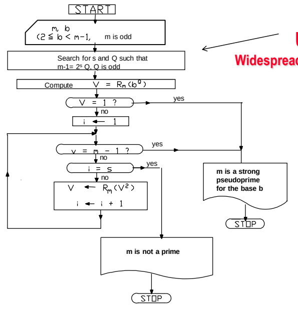
Based on: Fermat´s Theorem

- **If p is a prime number then for any 1 < b < p** $\quad b^{p-1} = 1 \pmod{p}$

- ***Primality test:*** **If an integer m fulfils Fermat theorem condition for some random integer b,**
  That is; if $b^{m-1} = 1 \pmod{m}$
  then m is called a *pseudoprime* to the base b.

- The probability that ***m is not a prime*** is ≈ 2^{-1}
  Therefore, for ***t*** such successful random tests, this **probability is ≈ 2^{-t}**
- ***Miller test*** **:** an improved test used to check "pseudo-primality" based on Fermat theorem

How to Find Probable Primes?



Use Miller Test
Widespread faster primality test algorithm

Miller test **based on Fermat theorem. For t independent random choices of b and successful tests, the probability that m is not a prime is roughly** $\leq 4^{-t}$

How to Find Provably-Primes ?

Based on *Pocklington´s Theorem (1916)*

Pocklington's Theorem

Let $n = 1 + F\,R$ and let $F = q_1 \dots q_t$ be the distinct prime factors of **F**.
If there exists an integer **a** such that **all the following three conditions** hold,

1. $a^{n-1} \equiv 1 \pmod n$
2. for all q_i s where $i = 1 .. t$, $\gcd(a^{(n-1)/q_i} - 1, n) = 1$,
3. if $F > \sqrt{n}$,

then **n** is prime.

The probability that a randomly selected **a** satisfies Pocklington's Theorem is $(1 - \Sigma 1/qi)$

Example: n = 2 (3 • 11) + 1 = 67, F = 3 x 11 and R=2. Is 67 a prime?
Proof: select a=2 (1 < a < 67)
1. $2^{67-1} = 1 \mod 67$ (or in Z_{67}) is true
2. $\gcd(2^{(67-1)/3} - 1, 67) = \gcd(2^{22} - 1, 67) = 1$ is true (selecting a=2)
   $\gcd(2^{(67-1)/11} - 1, 67) = \gcd(2^{6} - 1, 67) = 1$ is true
3. $F = 3 \times 11 > \sqrt{67}$ => 33 > 8.18 is true => 67 is prime

By selecting R=3 => n = 3 (3x11) +1 = 100. Is 100 a prime?.
Check: condition 1: $2^{100-1} = 2^{99} = 88 \neq 1 \pmod{100}$ is not true, condition 2 : is not true => 100 is not a prime !

Setting up GF(67) Algebra

Some facts in GF(67)

1. Number of invertible elements in GF(67) is Euler function **ϕ(67) = (67-1)=66 = 2.3.11**
2. The possible multiplicative orders in GF(67) are the divisors of 66 namely **1, 2, 3, 6,11,22,33,66**
   Notice: Prime factors of 66 are known when constructing the prime 67 = $\underbrace{2 \times (3 \times 11)}_{66 = 2.3.11}$ + 1
3. Number of elements with order 1 is **ϕ(1) = 1**
   Number of elements with order 33 is **ϕ(33) = ϕ(3x11)=(3-1) (11-1)= 20**
   Number of elements with order 66 is **ϕ(66) = ϕ(2x3x11)=(2-1)(3-1)(11-1)= 20**
4. **Example: order of 11:** $11^1 = 11 \neq 1$, $11^2 = -13 \neq 1$, $11^3 = -9 \neq 1$, $11^6 = 14$, $11^{11} = 30$, $11^{22} = 29 \neq 1$,
   $11^{33} = 29 \times 11 = -1 \neq 1$ => **order of 11 is 66.**
   Now we know that the order of 11 is 66 , thus **Ord (11^i) = 66 / gcd (66,i).**
   by selecting i=2 => order [11^2=54]= 66/2=33.
   by selecting i=5 => order [11^5=50]=66/1=66.
   by selecting i=6 => order [11^6 =14]= 66/6=11.

Mult. Inv of **31** in GF(**67) =13**

n_1	n_2	a_1	b_1	a_2 (a_1-qa_2)	b_2 (b_1-qb_2)	q	r	computation
67	31	1	0	0	1	2	5	67/31 =2 + 5/67
31	5	0	1	1	0-2x1 -2	6	1	31/5= 6 +1/5
5	1	1	-2	---	1-6x-2 13	5	0	5/1=5+ 0/1

Special Useful Primes

Strong Primes
A prime number p is said to be a strong prime if (p-1) has a large prime factor q, in best case p -1 = 2q (that is p=2q+1)
Example: p=23, p-1 = 22 = 2 x 11, that is q=11.

Mersenn Primes
Are primes having the form 2^k-1 in binary form k 1's $\overbrace{1111\dots1111}^{\text{k time 1's}}$
Known Primes for k= 2, 3, 5, 7, 13, 17 ..... 82 589 933 (status 2018)

Primes in the form $2^k + 1$ in binary form $\overbrace{10000 \dots 0001}^{\text{k-1 time 0's}}$, *(k+1 bits)*
Are primes with practical importance known for k= 0, 1, 2, 4, 8, 16
Example: (2^{16} +1) is a prime used in practical crypto-systems

Special Useful Primes

Strong Primes
A prime number p is said to be a strong prime if (p-1) has a large prime factor q, in best case p -1 = 2q
Example: p=23, p-1 = 22 = 2 x 11, that is q=11.

Mersenn Primes
Are primes having the form 2^k-1 in binary form k 1's $\overbrace{1111\dots1111}^{\text{k time 1's}}$
Known Primes for k= 2, 3, 5, 7, 13, 17 ..... 82 589 933 (status 2018)

Primes in the form $2^k + 1$ in binary form $\overbrace{10000 \dots 0001}^{\text{k-1 time 0's}}$, *(k+1 bits)*
Are primes with practical importance known for k= 0, 1, 2, 4, 8, 16
Example: (2^{16} +1) is a prime used in practical crypto-systems

Special Useful Primes

Fermat Primes
Having the form: $2^{2^n} + 1$
Example: exist for: $n \in \{0,1,2,3,4,?\}$

Permutable prime
is a prime with at least two distinct digits which remains prime on every rearrangement (permutation) of the digits:
Example: **337, 373, 733** are all primes (in the decimal system, base 10)

Palindromic Prime
Example of a pyramid of palindromic primes:

2
30203
133020331
1713302033171
12171330203317121
151217133020331712151
1815121713302033171215181
16181512171330203317121518161
331618151217133020331712151816133

Hardware Complexity of Modular Multipliers with Special Primes

Example when using Mersenn prime as modulus:

- If the modulus is a Mersenn p where p = 2^k-1 then 2^k-1 = 0 mod p, therefore **2^k = 1 mod p**
- An integer X having 2k-bits can be written as:

X = a + 2^k b

a (k-bits)	2^k b

← X →

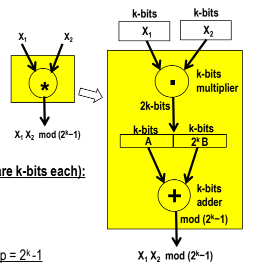
Then: **X mod p = a + b**

The modular product of $X_1 \cdot X_2$ (where X_1, X_2 are k-bits each):

If $X_1 \cdot X_2 = A + 2^k B$ (the product has 2k-bits)

Then **$(X_1 X_2) \bmod p = A + B$**
No need for division to compute the remainder modulo p = 2^k-1

Hardware implementation



Special Practically Standardized Primes

!!!! Primes represent still a big scientific mystery with serious impact on mdern everday's life!!!!!

The five NIST primes are:

$p_{192} = 2^{192} - 2^{64} - 1$

$p_{224} = 2^{224} - 2^{96} + 1$

$p_{256} = 2^{256} - 2^{244} + 2^{192} + 2^{96} - 1$

$p_{384} = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

$p_{521} = 2^{521} - 1$

The largest prime p_{521}, is a Mersenne prime, and the rest are generalized Mersenne primes.
Except for p_{521}, the exponents of 2 in the NIST primes are all **multiples of 32 or 64**.
This leads to efficient tricks for arithmetic modulo such primes executed on 32-bit or 64-bit computers.

secp256k1 is used for Bitcoin operating over GF(*p*)

Where p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F (in HEX)

$p = 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1$

Golden primes and Goldilocks for Elliptic-Curve systems ED448:

(by Mike Hamburg)

The prime in this case is $p = 2^{448} - 2^{224} - 1$ called the **"Goldilocks" prime**. In the form $p = \varphi^2 - \varphi - 1$ where $\varphi = 2^{224}$. The middle term 2^{224} is just the right size. Because 224 = 32*7 = 28*8 = 56*4, this prime supports fast arithmetic in radix 2^{28} or 2^{32} (on 32-bit machines) or 2^{56} (on 64-bit machines).

Modular Multiplication Complexity for ED448 modulus

Golden primes and Goldilocks for Elliptic-Curve ED448: (by Mike Hamburg)
The prime $p = 2^{448} - 2^{224} - 1$ is used as modulus in GF(p). Where $p = \varphi^2 - \varphi - 1$ and $\varphi = 2^{224}$

As p is the modulus, $p = \varphi^2 - \varphi - 1 = 0$ *therefore =>* $\varphi^2 = \varphi + 1$ *and* $\varphi = 2^{224}$

X_1 and X_2 are two integers each having 448-bits and can be describes as follows:

$X_1 = (a + \varphi b)$ *a and b are two 224-bits integers,*

224-bits	224-bits
a	2^{224} b

$X_2 = (c + \varphi d)$ *c and d are two 224-bits integers*

224-bits	224-bits
c	2^{224} d

The product of the two 442-bit integers $X_1 \bullet X_2$ mod p can be computed as follows:

$$X_1 \bullet X_2 = (a + b\varphi) \bullet (c + d\varphi) = ac + (ad + bc)\varphi + bd\,\varphi^2$$

$$\begin{aligned} X_1 \bullet X_2 \bmod p &\equiv ac + (ad + bc)\varphi + bd\,\varphi^2 \bmod p \\ &\equiv ac + (ad + bc)\varphi + bd(\varphi + 1) \\ &\equiv ac + bd + (ad + bc + bd)\varphi \\ &\equiv ac + bd + (ad + bc + bd + ac - ac)\varphi \\ &\equiv ac + bd + (ad + bc + bd + ac - ac)\varphi \end{aligned}$$

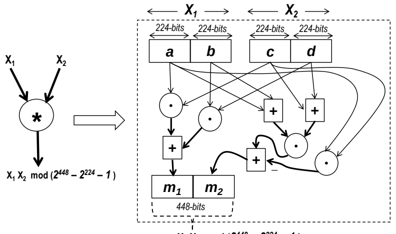
$$X_1 \bullet X_2 \bmod p \equiv (ac + bd) + \varphi\,[(a + b)(c + d) - ac]$$

Complexity: four 224-bits multiplications and four 224-bit additions/subtractions

Example: Tricky ED448 Modular Multiplier Construction: (by Mike Hamburg)

The prime $p = 2^{448} - 2^{224} - 1$ is used as modulus. Where $p = \varphi^2 - \varphi - 1$ and $\varphi = 2^{224}$

Constructing a computation structure for: $X_1 \bullet X_2 \bmod p \equiv \underbrace{(ac + bd)}_{m_1} + \varphi\,\underbrace{[(a + b)(c + d) - ac]}_{m_2}$



$X_1 X_2 \bmod (2^{448} - 2^{224} - 1)$