CREATIVE MATH. & INF.
16 (2007), 20 - 26

Dedicated to Professor Ioan A. RUS on the occasion of his 70^{th} anniversary

Some primality and factoring tests

CRISTINA FLAUT

ABSTRACT. In this paper we try to give some properties of strong pseudo-prime numbers and their applications in cryptography and algebra, more precisely in the factorization in $\mathbb{Z}[i]$.

1. INTRODUCTION

The Miller-Rabin test

Proposition 1. *Let $p > 2$ be a prime number and let $p - 1 = 2^t s$, with s an odd number. Let $a \in \mathbb{Z}$, $\gcd(a, p) = 1$. Then $a^s \equiv 1 mod\, p$ or there is an integer $k, 0 \leq k < t$ such that $a^{2^k s} \equiv -1 mod\, p$.*

Proof. Let $a_k = a^{2^k s} mod\ p, 0 \leq k \leq t$. From Fermat's Little Theorem, we have $a_t \equiv 1\, mod\ p$. Then we have
i) $a_k \equiv 1 mod\, p$, for all k; or
ii) There is $k \in \{1, 2, ..., t-1\}$, $p \nmid (a_k - 1)$ and $a_{k+1} \equiv 1 mod\, p$.
Then we have $a_{k+1} = a_k^2 \equiv 1 mod\, p$. So that $a_k \equiv -1 mod\, p$. □

Proposition 2. *Let n be an odd integer and $n - 1 = 2^t s$, with s an odd number. If we found an element $a \in \mathbb{Z}, 2 \leq a \leq n-1$, such that $n \nmid (a^s - 1)$ and $n \nmid (a^{2^k s} + 1)$, for all $k \in \{1, 2, ..., t-1\}$, then n is not a prime element.*

The algorithm

Input: N an odd integer to test for primality.
Output: Composite, if N is composite, otherwise N could be prime.

1) Let N be an odd integer. Write $N - 1 = 2^t s$.
2) We choose randomly an integer a such that $1 < a < N$. If, for all k, $N \nmid (a^s - 1)$ and $N \nmid (a^{2^k s} + 1)$, then N is composite. Otherwise, N is probably prime.

Remark 1. The running time of this algorithm is $O(k \times \log^3 N)$, where k is the number of different value of a which we test. Unfortunately there are the numbers which pass the test and they are composite. In [1], we found a number which is not prime and passes the Miller-Rabin test for the basis a,

$$a \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\} :$$

Received: 10.09.2006. In revised form: 10.01.2007.
2000 *Mathematics Subject Classification.* 11A41, 1A51, 11R04.
Key words and phrases. *Pseudo-prime numbers, strong pseudo-prime numbers, Miller-Rabin test.*

$$N = 1195068768795265792518361315725116351898245581 =$$
$$= 24444516448431392447461 \cdot 48889032896862784894921.$$

In [1] it is shown that a composite number could passes the Miller-Rabin test for at most $1/4$ of the possible bases a.

Definition 1. Let N be an odd integer. If $N-1=2^t s$, with s an odd number, then the number N is called a **strong pseudo-prime** number in basis a, with $\gcd(a,N)=1$, if $a^s \equiv 1 mod\, N$ or there is an integer $k, 0 \leq k < t$ such that $a^{2^k s} \equiv -1 mod\, N$.

In the next, we give a procedure, with Maple, for finding the small strong pseudo-prime numbers in basis a, with $a \in \{2,4,5,6,7,8,9,10\}$.

```
rm:=proc(nn,a)local s,t,r,m,q,z,v,i; s:=nn-1:t:=0:r:=1: for i from
1 to nn do if s mod 2=0 then t:=t+1:s:=s/2:fi:od: r:=(nn-1)/2^t:
m:=0:q:=0:m:=-1 mod nn:z:=0:q:=a^r mod nn: if q=1 then RETURN(1)
:fi: if q<>1 then for i from 0 to t-1 do v:=(a^(r*(2^i)))mod nn:
if v=m then z:=z+1:fi:od:if z<>0 then  RETURN(1):fi:fi:end:
```

We test this procedure for $a=2$. Then we have:

```
a:=2: for nn from 2 to 10000 do if gcd(nn,a)=1 and rm(nn,a)=1 and
isprime(nn)=false then print(nn):fi:od:
                                 2047
                                 3277
                                 4033
                                 4681
                                 8321
```

In the same way, for $a=3$, we have $N \in \{121, 286, 703, 1891, 3281, 8401, 8911\}$. For $a=4$,we get $N \in \{341, 1387, 2047, 3277, 4033, 4371, 4681, 5461, 8321, 8911\}$. For $a=5$, we obtain $N \in \{4, 124, 781, 1541, 5461, 5611, 5662, 7813\}$. For $a=6$, we have $N \in \{217, 481, 1111, 1261, 2701, 3589, 5713, 6533\}$. For $a=7$, we get $N \in \{6, 25, 325, 703, 2101, 2353, 4525\}$. For $a=8$, we obtain $N \in \{9, 65, 481, 511, 1417, 2047, 2501, 3277, 3641, 4033, 4097, 4681, 8321\}$. For $a=9$, we have $N \in \{4, 8, 28, 52, 91, 121, 286, 364, 532, 616, 671, 703, 946, 1036, 1288, 1541, 1729, 1891, 2806, 2821, 2926, 3052, 3281, 3367, 3751, 4376, 4636, 5356, 5551, 6364, 7381, 8401, 8744, 8866, 8911\}$. For $a=10$, we get $N \in \{9, 91, 1729, 4187, 6533, 8149, 8401\}$.

Definition 2. Let N be an odd integer. The number N is called a **pseudo-prime** number in basis a, with $\gcd(a,N)=1$, if $a^{N-1} \equiv 1 mod\, N$.This number passes the Fermat test.

Proposition 3. *a) There are infinitely many strong pseudo-primes for the basis* 2.
b) If n *is a strong pseudo-prime in basis* a, *then* n *is a strong pseudo-prime in basis* $a^i, \forall i \in \mathbb{N}$.

Proof. a) First of all, we prove that if n is a pseudo-prime number in basis 2, then the number $N = 2^n - 1$ is a pseudo-prime in basis 2. Indeed, $N - 1 = 2(2^{n-1} - 1)$. Since $2^{n-1} \equiv 1 \; mod \; n$, then $n \mid 2^{n-1} - 1$, hence $n \mid N - 1$ therefore $N - 1 = nq$. Since $2^n \equiv 1 mod \; N$, we have $2^{N-1} \equiv 1 mod \; N$, then is pseudo-prime. It follows that we have an infinitely pseudo-primes in basis 2. We prove that N is a strong pseudo-prime in basis 2. With the notation from the Proposition 1., we have $t = 1$ and $s = 2^{n-1} - 1$. Then N is a strong pseudo-prime in basis 2 if and only if either $2^s \equiv 1 mod \; N$ or there is an integer $k, 0 \leq k < t$ such that $2^{2^k s} \equiv -1 mod \; N$. For $k = 0$, we have $2^s \equiv \pm 1 mod \; N$.

b) Suppose that $n - 1 = 2^t s$, with s an odd number. If $a^s \equiv 1 mod \; n$, then $(a^s)^i \equiv 1 mod \; n$. If $a^{2^k s} \equiv -1 mod \; n$, for an integer $k, 0 \leq k < t$, then if $i = 2^r q, q$ being an odd number, we have the possibilities:

i) $r > k$, then $(a^i)^s \equiv 1 mod \; n$;

ii) $r \leq k$, then $(a^i)^{2^{k-r} s} = (a^{2^k s})^q \equiv (-1)^q = -1 mod \; n$.□ □

The Lehman test

This algorithm finds a non-trivial factor for a natural number n or finds if this number is a prime number.

The algorithm.[1]

Input: $n \in Z$.
Output: factorization of n.

1) We put $B = [n^{\frac{1}{3}}]$. We find, to the bound B, a nontrivial factor. If we found a factor, the algorithm stops here. Otherwise, let $k = 0$.

2) Let $k = k + 1$. If $k > B$, then n is prime and stop the algorithm. Otherwise, let $r = 1$ and $t = 2$ if k is even, $r = k + N$ and $t = 4$ if k is odd.

3) For all natural numbers x such that $4kn \leq x^2 \leq 4kn + B^2$ and $x \equiv r \; mod \; t$, let $z = x^2 - 4kn$. If $z = y^2$, $y \in \mathbb{N}$, then the $\gcd(x + y, n) = w, w$ is a factor of n. Otherwise, use the next value of x. If all possible values of x are tested, then go to step 2.

Remark 2. If the smallest prime factor p of the natural number n has the property $p^3 > n$ and $n = pq$, then q is a prime number. In the above algorithm, if we find the smallest p which is a prime factor of n, such that $p^3 > n$, then we stop the algorithm and we find the factorization of n.

2. APPLICATIONS

2.1. Application in cryptography

Proposition 4. [4] *If we find a basis a such that the odd number N is a pseudo-prime but not a strong pseudo-prime in basis a, then we can find quickly a non-trivial factor of N.*

Proof. If N is a pseudo-prime number then $a^{N-1} \equiv 1 mod\ N$. If N is not a strong pseudo-prime in basis a, we have that there is an integer $k, 0 < k < t$ such that $a^{2^k s} \equiv 1 mod\ N$, where $N - 1 = 2^t s$, and s an odd number. Let $b = a^{2^k s}$, then $b^2 \equiv 1 mod\ N$. We have $N \mid (b^2 - 1)$ hence $\gcd(b+1, N) = d > 1$. □

Remark 3. In RSA cryptosystem the module N is chosen such that N is a strong pseudo-prime. From Proposition 4., if a composite number passes the Fermat test and it is not a strong pseudo-prime number, then we find that this is a composite number, we find its divisors and we break the cryptosystem.

2.2. Application in algebra

From Proposition 4., we have that, if the number n is pseudo-prime and it is not strong pseudo-prime, then this number is composite. In the next, we try to apply the Miller-Rabin test to detecting the prime numbers in the Euclidean ring $\mathbb{Z}[i]$. In the Euclidean ring $\mathbb{Z}[i]$, we have the norm function

$$\varphi : \mathbb{Z}[i] \to \mathbb{N},\ \varphi(z) = a^2 + b^2, \text{ where } z = a + bi,\ a, b \in \mathbb{Z}.$$

This function φ has the properties:

1) $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$.

2) If $\varphi(z) = p$, where $p \in \mathbb{Z}$ is a prime number in $\mathbb{Z}$, then z is a prime number in $\mathbb{Z}[i]$.

Proposition 5. [5] *i) If p is a prime number, $p = 4k+1$ then p is a sum of two squares.*
ii) If $p = a^2 + b^2 = x^2 + y^2, x \neq a, x \neq b, y \neq a, y \neq b$, then p is composite.
iii) If $p \in \mathbb{Z}$ has the form $p = 4k + 3$, and p is prime in $\mathbb{Z}$, then p is prime in $\mathbb{Z}[i]$.
iv) If an odd number $n \in \mathbb{N}$ is a sum of two non zero square, then it has the form $4k+1$.

Proof. i) By Wilson Theorem, we have :

$$\begin{aligned} p-1 &\equiv -1\, modp \\ p-2 &\equiv -2\, modp \\ &\ldots\ldots\ldots\ldots\ldots \\ \frac{p-1}{2}+1 &\equiv -\frac{p-1}{2}\, modp. \end{aligned}$$

We obtain $1 + x^2 \equiv 0\ modp$, with

$$x = \left(\left(\frac{p-1}{2}\right)!\right)^2.$$

It results that

$$p \mid (1+ix)(1-ix).$$

If p is a prime number in $\mathbb{Z}[i]$, then $p \mid (1+ix)$, or $p \mid (1-ix)$, false. Then $p = \pi_1\pi_2....\pi_t$, where $\pi_i \in \mathbb{Z}[i]$ are prime elements for $t \geq 2$. Since $p^2 = \varphi(p) = \varphi(\pi_1)....\varphi(\pi_t)$, we have $t \leq 2$, then $p = \pi_1\pi_2$, $\pi_1 \neq \pi_2$ and π_1 is not associate with π_2. In this case $\pi_1 = a+ib, \pi_2 = a-ib$, then $p = a^2+b^2$.

ii) If

$$p = a^2+b^2 = x^2+y^2, x \neq a, x \neq b, y \neq a, y \neq b,$$

we have

$$a^2 - x^2 = y^2 - b^2 \Rightarrow (a-x)(a+x) = (y-b)(y+b).$$

If a and x are odd numbers and b and y are even numbers then

$$\frac{a-x}{y-b} = \frac{y+b}{a+x} = \frac{q}{r}.$$

Then we have $a-x = sq$, $y-b = sr$ and $y+b = wq$, $a+x = wr$. We obtain $a = \frac{1}{2}(sq+wr)$, $b = \frac{1}{2}(sr+wq)$ and $n = a^2+b^2 = \frac{1}{4}[(sq+wr)^2+(sr+wq)^2] = \frac{1}{4}(q^2+r^2)(s^2+w^2), s, w \in \mathbb{Z}$. □

Proposition 6. *Let n be an odd natural number such that $n = a^2+b^2$ in a unique way. Then n is a prime number or it has only one factor of the form $4k+1$ at power one and the other factors are even power of prime number of the form $4k+3$.*

Proof. We suppose that n is not a prime number. Then its prime factors are the form $4k+3$ or $4k+1$. Let $p_1 = a_1^2+b_1^2$ and $p_2 = a_2^2+b_2^2$ two prime divisors of n. Then $p_1p_2 = \left(a_1^2+b_1^2\right)\left(a_2^2+b_2^2\right) = a_1^2a_2^2 + a_1^2b_2^2 + b_1^2a_2^2 + b_1^2b_2^2 + 2a_1a_2b_1b_2 - 2a_1a_2b_1b_2 = (a_1b_2+b_1a_2)^2 + (a_1a_2-b_1b_2)^2 = (a_1b_2-b_1a_2)^2 + (a_1a_2+b_1b_2)^2$. Since we have a unique writing of n like a sum of two squares, we obtain that $b_1a_2 = 0$ and $b_1b_2 = 0$ or $a_1b_2 = a_1a_2$. From the first, we have that $b_1 = 0$, false, from the second we have that $a_1 = 0$, or $b_2 = a_2$, false. So that, if n are prime divisors only of the form $4k+1$, then n has a two distinct writings like a sum of two non-zero square. Then, we have divisors of the form $4k+3$ and only one of the form $4k+1$, at power one. Since n is a sum of two squares, the prime divisors of the form $4k+3$ have even power. Indeed, if the prime factors have the form $(4k+3)$ and $(4t+3)$ at power one, then we have $a^2+b^2 = (4k+3)(4t+3)$. We obtain that $(4k+3)$, is prime in $\mathbb{Z}$ and in $\mathbb{Z}[i]$, and divides $a^2+b^2 = (a+bi)(a-bi)$ in $\mathbb{Z}[i]$, so that $(4k+3) \mid (a+bi)$. It follows $(4k+3) \mid a$ and $(4k+3) \mid b$, so that $(4k+3)^2 \mid a^2+b^2$, false. □

Remark 4. For a composite number n, like in the above proposition, we observe that this number has the prime factors smallest than $n^{\frac{1}{3}}$. Indeed, if $n = p^2q, p = 4k+3, q = 4k+1$ are prime and $p > n^{\frac{1}{3}}, q > n^{\frac{1}{3}}$, then $n = p^2q > n^{\frac{1}{3}}n^{\frac{1}{3}}n^{\frac{1}{3}} = n$, false. That factor we can find quickly. If, for n odd, such that n is written like a sum of two non-zero squares, in a unique way, we don't find a prime factor less than $n^{\frac{1}{3}}$, then n is a prime number.

If we apply the Miller-Rabin test we obtain the composite numbers passing the test. We observe that in our case, we apply this test to odd numbers which are sums of two squares, so that they have the form $4k+1$. From Proposition 5. ii), we test whether these numbers could be write as a sum of two square in two different ways. In this case these numbers are composite and, from above proposition, we have their factorization. First, we verify if n is a square, $n = m^2$. If $m = 4k+3$ is prime then we have that $z = m$ or $z = mi$, is prime in $\mathbb{Z}[i]$. Otherwise, z is a composite.

The Algorithm

1) We apply the Miller-Rabin test to the number n which is not a square. If the test return *composite*, then n is composite and z is not a prime element in $\mathbb{Z}[i]$. Otherwise, go to the step 2).

2) If n is not a square, we test if n could be write as a sum of two squares in two different ways. If the answer is positive, then n is composite in $\mathbb{Z}$ and z is composite in $\mathbb{Z}[i]$ and we have their factorization. Otherwise, n could be prime and z is prime, or n has a only prime divisor of the form $4k+1$, and the other factors are the even power of prime numbers of the form $(4k+3)$, so that z is not a prime element. Using the above remark, we choose the prime factors less than $n^{\frac{1}{3}}$. If we don't find then n is a prime number.

We can use the Lehman test for the factorization of the number n, $n = p_1^{\alpha_1}...p_t^{\alpha_t}$ By the Proposition 6., we have that $p_j = (a_j+b_ji)(a_j-b_ji)$ (p_j has the form $4s+1$), or $p_j = 4k+3$ and α_j is even. Then z is of the form $z = i^{\beta_1}\prod_{j=1}^{t}(a_j \pm b_ji)^{\alpha_j}$. For "$\pm$", we verify if $(a_j+b_ji) \mid z$ or $(a_j-b_ji) \mid z$.

Example. Let $z_1 = 57+70i$, $z_2 = 7+90i$. We have $\varphi(z_1) = \varphi(z_2) = 8149$. Let $n = 8149$. Now, if we use the Miller-Rabin test, n passes the test for the basis 10.

```
n:=8149:s:=n-1:t:=0:r:=1: for i from 1 to n do if s mod 2=0
 then t:=t+1:s:=s/2:fi:od: r:=(n-1)/2^t:print(t):print(r):
                              2

                             2037

a:=10:m:=0:q:=0:m:=-1 mod n:z:=0:q:=a^r mod n: if q=1 then
print('IS PRIME'):fi: if q<>1 then for i from 0 to t-1 do
 v:=(a^(r*(2^i)))mod n:if v=m then z:=z+1:fi:od:
if z=0 then print('IS NOT PRIME') else
 print('IS PRIME'):fi:fi:

                           IS PRIME
```

Then we use the Miller-Rabin test for $\mathbb{Z}[i]$, and, with Maple, we obtain:

```
mm:=sqrt(n):if type (mm,integer) then print('is a square'):
 else ki:=0:for ii from 1 to n do  jj:=n-ii^2:
  if ii^2< n and type (sqrt(jj),integer) then
```

```
    print(ii):ki:=ki+1 :fi:od:
 if ki>=4 then print('is not prime') else
   print ('is prime'):fi:fi:

                                  7
                                  57
                                  70
                                  90
a:=7;b:=90;x:=57;y:=70;s:=gcd(x-a,b-y);
q:=(x-a)/s;r:=(b-y)/s;w:=gcd(y+b,x+a);
n1:=(q^2+r^2);n2:=1/4*(s^2+w^2);n:=n1*n2;
                                    a := 7
                                   b := 90
                                   x := 57
                                   y := 70
                                   s := 10
                                    q := 5
                                    r := 2
                                   w := 32
                                   n1 := 29
                                  n2 := 281
                                  n := 8149
```

Then we obtain that n is not prime in $\mathbb{Z}$ and that z_1 and z_2 are not prime in $\mathbb{Z}[i]$. We factorize $n, n = 29 \cdot 281$, with $29 = 4 + 25$ and $281 = 25 + 256$ $prime$ numbers. Then, for example, $z_1 = i^{\beta_1}(2 \pm 5i)(5 \pm 16i)$. We test either if $2 + 5i$ divides n or $2 - 5i$ divides n. We have $2 + 5i \mid n$ and $5 + 16i \mid n$. Then $z_1 = i^3(2 + 5i)(5 + 16i)$.

References

[1] Cohen H., *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1995

[2] Grossman P., *Discrete mathematics for computing*, Palgrave Macmillan, New-York, 2002

[3] Guy R. K., *Unsolved problems in number theory*, Springer-Verlag, New-York, 1994

[4] Koblitz N., *A course in number theory and cryptography*, Springer-Verlag, New-York, 1994

[5] Năstăsescu C., Niţă C. and Vraciu C., *Bazele algebrei*, Editura Academiei, Bucureşti, 1986

University "Ovidius"
Department of Mathematics and Informatics
Bd. Mamaia 124
900527 Constanta, Romania
E-mail address: cflaut@univ-ovidius.ro
E-mail address: cristina_flaut@yahoo.com