

Re: Proving primality of an integer

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-02/2225.html>

From: Aldo (gasparuga@yahoo.ca)

Date: 02/10/03

From: gasparuga@yahoo.ca (Aldo)

Date: 9 Feb 2003 15:10:43 -0800

"Cristiano" <cristiano.pi@nsquipo.it> wrote in message
news:<XTq1a.208195\$AA2.8166443@news2.tin.it>...

>
> *Just a question: if your program say "N is prime", N is really prime*
> *without any doubt?*
>

In general only if AKS Conjecture 4 is true.
So far nobody found an exception. If one could be found then AKS
conjecture 4 would proven false and "primes" proven by it would
be some sort of pseudoprimes.
Other way is to prove Conjecture 4 true and make of it a theorem.

Your translation of the program into C++ is very good.

> *This is my translation in c++ for miracl (N.get_bit() is not included in*
> *the miracl library):*
>
> // -----
> // (S(x)*S(x)) % (x^r-1) % n
> // -----
> void S_x_S(Big *S,Big *T,const int R,Big &N)
> {
> for(int i=0;i<=R;i++) { S[i]=T[i]; T[i]=0; }
>
> for(int i=0;i<R;i++)
> for(int j=0;j<R;j++) {
> int k=(i+j)%R; T[k]=(T[k]+S[i]*S[j])%N;
> }
> }
>
> // -----
> // (S(x)*A(x)) % (x^r-1) % n
> // -----
> void S_x_A(Big *S,Big *T,const int R,int *A,Big &N)

```

> {
> for(int i=0;i<=R;i++) { S[i]=T[i]; T[i]=0; }
>
> for(int i=0;i<R;i++)
> for(int j=0;j<=1;j++) {
> int k=(i+j)%R; T[k]=(T[k]+S[i]*A[j])%N;
> }
> }
>
> int AKS(Big &N)
> {
> int R=2,K=N%R;
> while(K*K%R==1) { R++; K=N%R; }
>
> if(K==0) return 0; // N is divisible by R
>
> Big *S=new Big[R+1],*T=new Big[R+1];
> int A[2]={-1,1}; // A = x-1
>
> T[0]=-1; T[1]=1;
>
> // Mod exp: (x-1)^n (mod x^r-1, n)
> // -----
> int I=bits(N)-2;
> while (I>=0) {
> S_x_S(S,T,R,N); // (S*S)%(x^r-1)%n
> if(N.get_bit(I)) S_x_A(S,T,R,A,N); // (S*A)@(x^r-1)@n
> I--;
> }
>
> // Normalization as in UBASIC
> for(int i=0;i<=R;i++) if(T[i]<0) T[i]+=N;
>
> // -----
> // Test result
> // -----
>
> for(int i=0;i<=R;i++) S[i]=0;
> S[K]=1; S[0]=N-1;
>
> I=0; while (I<R && S[I]==T[I]) I++;
>
> delete[] S; delete[] T;
>
> if(I==R) return 1; // N is prime
> return 0; // N is composite
> }
>
> Cristiano

```

I will only add a new simplification to the test routine:

sci.crypt: Re: Proving primality of an integer

```
530 ' Test result
540 ' -----
550 block ema(S;*,0)=0
560 ema(T;K,0)--=1
570 ema(T;0,0)--=N-1
580 '
590 I=0
600 while and{I<R,ema(T;I,0)=0}
610 inc I
620 wend
630 '
640 if I=R then print "N is prime"
650 :else print "N is composite"
660 end
```

There is more I have to say about my program.
I hope to find some time and post more stuff soon.

Thank you for taking time to read and understand my post.

Regards,

Aldo D.