Primality of Repunit
A small reduction of the exponent

ver. 1.0 - Jan 2011

Giovanni Di Maria
93100 Caltanissetta – Sicilia
Italia

email: calimero22@yahoo.it

Abstract

A repunit is a number consisting of copies of the single digit 1. Examples of repunit are 11, 1111, 11111. A repunit prime is a repunit that is also a prime number.

In base 10, repunits have the form: $\frac{(10^p-1)}{9}$ where p is a prime number.

Usually, people use Fermat's little theorem, to test the pseudo-primality of Repunit numbers. I remember that this theorem states that if p is a prime number, then for any integer a, a^$p-a$ will be evenly divisible by p. This can be expressed in the notation of modular arithmetic as follows:

$$a^{Rp} \equiv a \left(mod\ Rp \right)$$

A variant of this theorem is stated in the following form: if p is a prime and a is an integer coprime to p, then a^$(p-1)-1$ will be evenly divisible by p. In the notation of modular arithmetic:

$$a^{Rp-1} \equiv 1 \left(mod\ Rp \right)$$

<u>In this paper, i show that the exponent can be reduced a bit.</u>

1 Introduction

1) Let p be a prime number;
2) Let Rp be $\frac{(10^p-1)}{9}$ (Repunit);

In order to reduce the exponent, i can say that Rp is a probable prime number if:

$$2^{\frac{Rp-1}{2\mathrm{p}}} \equiv 10^n (mod\ Rp)$$

where $n \in \{1..\mathrm{p}\}$

In other words, i can say that:

- If the residual is in the form 10^n (where $1 \leq n \leq p$), then Rp is a probable prime number;
- If base-10 logarithm of the residual is integer, then Rp is a probable prime number.

2 Results

Now i show you the residuals of the formula:

$$2^{\frac{Rp-1}{2p}} \equiv 10^{n} \left(mod\ Rp \right)$$

on known Repunit Primes (and probable primes) in the following table.

R_p	$2^{\frac{Rp-1}{2p}}\ mod\ Rp$	**Expansion**
R_{19}	10^{8}	100,000,000
R_{23}	10^{12}	1,000,000,000,000
R_{317}	10^{62}	100............00000 Too large to show
R_{1031}	10^{697}	100............00000 Too large to show
R_{49081}	10^{46706}	100............00000 Too large to show
R_{86453}	10^{22373}	100............00000 Too large to show
R_{109297}	10^{92105}	100............00000 Too large to show
R_{270343}	10^{183100}	100............00000 Too large to show

3 Comparative table of the exponents

I compare here the size of exponents, represented in binary notation. In other words, i count the number of bits.

The two formulas to compare are:

$$a^{Rp} \equiv a \left(mod\ Rp \right)$$

versus

$$2^{\frac{Rp-1}{2p}} \equiv 10^{n} \left(mod\ Rp \right)$$

R_p	Size of exponent Rp (number of bits)	Size of exponent $\frac{Rp-1}{2p}$ (number of bits)	Bits saved
R_{19}	60	55	5
R_{23}	74	68	6
R_{317}	1050	1041	9
R_{1031}	3422	3411	11
R_{49081}	163041	163024	17
R_{86453}	287188	287171	17
R_{109297}	363074	363056	18
R_{270343}	898057	898038	19

4 Conclusions

By this formula, saving time and calculations is very small. It does not help to solve the problems of primality. However, i have found a way to reduce the exponent a bit. Excuse my English, not very good, but I'm Italian.

Good luck to all.

Giovanni Di Maria
Caltanissetta, Jan 3, 2011