Modular Arithmetic and Internet Encryption Day

25th January 2011

Jan 25-07:52

http://www.youtube.com/watch?v=xt3S29F_HII

Jan 13-14:20

The RSA Challenges

The RSA organisation have set the following challenge:

- they give you a number and you have to find two smaller numbers whose product gives the original number;
- if they agree with your result then they will pay you up to $200,000;
- they want to know, though, how you did it!

If they had given 15 as the challenge then
$15 = 3 \times 5$,
so 3 and 5 would be the answer.

The RSA numbers are, though, a bit bigger than this.

RSA-129
114381625757888867669235779976146612010218
2967212428626256184293570693525733807830
5971235639587050589890751479929002686794 3
541
Solved in 1994

RSA-155
109417386415705274218097073220405 76120037
329454492059909138421314763499842889347847
179972578912673324976257528997818337970765
372440271467435159335433389 7
Solved in 1999

RSA-174
188198812920607963838697239461650439807163
563379417382700763356422988859715234665485
319060606504743045317388011303396716199692
321205734031879550656996221305168759307650
257059
Set 2001 Solved 3 December 2003 $10,000

Jan 13-13:06

RSA-617
251959084756578934940271832400483985714292821262040320277771378360436620207075955562640185258807844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203570rth $200,000

As we have seen, checking that you have the correct answer is simple – just multiply the two numbers together!

Yet the challenges are really hard:

- RSA-155 took roughly 8.4 years of total computer time (divided among thousands of computers);
- RSA-309 is expected to take approximately 1.6 billion times as long;
- by the same estimation, RSA-617 would take significantly longer than the age of the Universe!

Yet it is easy to multiply two 350 digit numbers.

Jan 13-13:07

Adi Shamir Ron Rivest Leonard Adleman

Jan 13-13:09

Modular Arithmetic

You use modular arithmetic all the time:

What will the time be 100 hours from now?

What day of the week will it be 100 days from now?

What day of the year will it be 10000 days from now?

$37 \equiv x \pmod 7$

$10 \equiv y \pmod 7$

Jan 13-13:12

If:

$a \equiv b \pmod{m}$

and

$c \equiv d \pmod{m}$

is it true that:

$a + c \equiv b + d \pmod{m}$?

Prove it.

Jan 13-14:30

Test and then prove that if:

$a \equiv b \pmod{m}$

and

$c \equiv d \pmod{m}$

then

$ac \equiv bd \pmod{m}$

Is it true that $a^n \equiv b^n \pmod{m}$?

Jan 13-14:36

Find the remainders when the following are divided by 7:

(a) 26×44

(b) 37^2

(c) $37^2 + 34^2$

(d) 23^{49}

(e) 1234^{2345}

Jan 13-14:40

A number is divisible by 9 if the sum of its digits is a multiple of 9.

Choose some multiples of 9 and explore what happens if the partitioned parts of the number are analysed using mod 9.

Can you extend your reasoning to produce a proof of the fact stated at the top of the page?

<http://sites.google.com/site/mathematicsnotebook/divisibilityrules/divisibility3/alternate-proof>

Jan 13-16:44

A logical extension of this thinking is that any number can be tested for divisibility by a given divisor by adding the digits together.

Jan 18-09:54