Imperial College London

How to factorise a large semiprime

Phil Ramsden

Imperial College London

How to factorise a large semiprime

when the person who supplied it has been a bit careless

Phil Ramsden

Imperial College London

First Year Computing coursework

Based on “RSA” secret codes

Used to be in Maple

Now the students use Python

Imperial College London

First Year Computing coursework

RSA secret codes are based on **semiprimes**: products of large primes.

Factorise my semiprime and you've cracked my cipher.

You crack my cipher: 100% for the coursework...

... even if you get zero on everything else.

I crack your cipher: 5% penalty.

Key computational facts

Easy to do arithmetic with large integers. E.g. in Mathematica:

339375868466565360807296042046982561489532253683855183308113901695264308933 * 2373608159598101575520842629420704353629907985981682358020544989201899842 61

805545330562931600742583708964472910025860129430328563616841858552178571249728645547159135953340469115664629180137932160605086481347962892923117035 13

Addition, subtraction, division also very quick.

Imperial College
London

Key computational facts

Easy to calculate **highest common factors**. E.g. in Mathematica:

GCD[805545330562931600742583708964472910025860129430328563616841858552178571249728645547159135953340469115664629180137932160605086481347962892923117035 13,
32188286315646108036480463271289804138872430377703459512786362774663012984283995649494795500413738558213453253889071952132014045041947112088025985 4089]

339375868466565360807296042046982561489532253683855183308113901695264308933

Key computational facts

Easy to check whether a number is prime. E.g. in Mathematica:

PrimeQ[623363185418993110162526398149564136828374416416774794824102847557364874008292284327300589315058735820776708619757860853555458184130786457053847934519]

True

PrimeQ[805545330562931600742583708964472910025860129430328563616841858552178571249728645547159135953340469115664629180137932160605086481347962892923117035 13]

False

Imperial College
London

Key computational facts

Easy to find the smallest prime larger than a given number. E.g. in Mathematica:

NextPrime[805545330562931600742583708964472910025860129430328563616841858552178571249728645547159135953340469115664629180137932160605086481347962892923117035 13]

805545330562931600742583708964472910025860129430328563616841858552178571249728645547159135953340469115664629180137932160605086481347962892923117035 01

Key computational facts

Hard to factorise a large integer. E.g. in Mathematica:

```
FactorInteger[80554533056293160074258370896447291002586012
94303285636168418585521785712497286455471591359533404691
15664629180137932160605086481347962892923117035 13]
```

would take *at least* a few million years.

My resources

I haven’t got a supercomputer.

I haven’t got fast software.

I’m not a number theorist (though I know some).

I’m not a cryptographer.

Imperial College London

My task

Around 200 submissions.

Close to the deadline, I get 30-40 submissions a day.

I can afford to spend about **two minutes** on each.

Still, I usually crack between 15 and 30.

How? Sneakiness!

First Example

**n=358293514403723123236760569947839836203723967118107943
657873969122887107842262418491260701347507767771742014417225344969366153678325466431 97**

Trick: does there exist r such that $n+r^2$ is a perfect square?

Yes: turns out $\sqrt{n+48^2}$ is equal to

598576239424622603551471924114422907373235403759772284023736992256116 9

Imperial College London

First Example

The primes are

p1=5985762394246226035514719241144229073732354037597722840237369922561169 **– 48** =

59857623942462260355147192411442290737323540375977228402373699225611 21

and

p2=5985762394246226035514719241144229073732354037597722840237369922561169 **+ 48** =

59857623942462260355147192411442290737323540375977228402373699225612 17

$$p_1 p_2 = (\sqrt{n+r^2} - r)(\sqrt{n+r^2} + r) = (n+r^2) - r^2 = n.$$

First Example

Moral: don't choose your two primes too close together...

... or, more generally, too close to a ratio of 1:1, 3:2, 4:3 etc.

Second Example

**n=989000000000000000000000000000000000000000000000000000
00000000000000000001310800000000000000000000000000000000
0000000000000000000000000000000000000018023**

Second Example

**n=989000000000000000000000000000000000000000000000000000
0000000000000000000131080000000000000000000000000000000000
0000000000000000000000000000000000000018023**

This looks like a quadratic in $10^{\text{something}}$.

Indeed: turns out it's

$989\times10^{150}+13108\times10^{75}+18023$.

Now, factorising integers is hard…

… but factorising quadratics is easy.

Imperial College London

Second Example

Factorising integers is hard, but factorising quadratics is easy:

$$989x^2 + 13108x + 18023 = (23x + 269)(43x + 67).$$

Primes are $23 \times 10^{75} + 269$ and $43 \times 10^{75} + 67$; that is:

> 23000000000000000000000000000000000000000000000000000000000000000000000269

and

> 43000000000000000000000000000000000000000000000000000000000000000000000067

Second Example

Moral: don't make your primes out of powers of 10.

(Student had found the smallest primes greater than $23\times10\uparrow75$ and $43\times10\uparrow75$ respectively.)

Even if you use *unequal* powers of 10, you're vulnerable.

Imperial College London

Third Example

n=109670147968019502125174448700046892180522097880573084963433946353460232709090402291818735532687540151792653657439582626252476131

The $\sqrt{n+r^2}$ trick doesn't work.

And it's not based on powers of 10.

However…

Third Example

Its “digits” in **base 17** are

3,7,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,9,6,15,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,4,3

Third Example

Its “digits” in **base 17** are

3,7,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,9,6,15,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,4,3

3,7,3 in base 17 is 989

9,6,15 in base 17 is 2718

1,4,3 in base 17 is 360

and the number is equal to

$989 \times 17 \uparrow 100 + 2718 \times 17 \uparrow 50 + 360.$

Imperial College London

Third Example

Now:

$989x^2 + 2718x + 360 = (23x + 60)(43x + 6)$.

Primes are $23 \times 17^{50} + 60$ and $31 \times 17^{50} + 6$; that is:

765903236839376822757267764772728766140926297209297574379476787

and

143190605148231319037228321240118856278521003391303459557902171 3

Third Example

Moral: don't make your primes out of powers of *any other single number*.

Fourth Example

n=6791120569169638352330335299100101321290842656611341201647728025943677645728255708010156739206564233562586084411139

Its "digits" in base 23 are

2,18,7,22,17,20,17,5,0,20,17,6,0,6,18,0,10,19,15,14,17,0,15,18,14,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6,5,21,22,
5,7,9,14,2,2,11,18,8,6,18,15,13,19,2,16,12,0,4,0,1,22

Fourth Example

n=67911205691696383523303352991001013212908426566113412016477280259436776457282557080101567392065642335625860844 11139

Its “digits” in base 23 are

2,18,7,22,17,20,17,5,0,20,17,6,0,6,18,0,10,19,15,14,17,0,15,18,14,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6,5,21,22,
5,7,9,14,2,2,11,18,8,6,18,15,13,19,2,16,12,0,4,0,1,22

Just one sequence of zeroes this time.

Imperial College London

Fourth Example

2,18,7,22,17,20,17,5,0,20,17,6,0,6,18,0,10,19,15,14,17,0,15,18,14,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,6,5,21,22,
5,7,9,14,2,2,11,18,8,6,18,15,13,19,2,16,12,0,4,0,1,22

2,18,7,22,17,20,17,5,0,20,17,6,0,6,18,0,10,19,15,14,17,0,15,18,14 in base 23 is 1343603974704253363529027889043777

6,5,21,22,5,7,9,14,2,2,11,18,8,6,18,15,13,19,2,16,12,0,4,0,1,22 in base 23 is 691345317893279457961299804726161 62

The **highest common factor** of these numbers is
122145815882204851229911626276707

Fourth Example

Highest common factor 1221458158822048512299116262767 07

That's our first prime! Get the second one by division.

679112056916963835233033529910010132129084265661134120164772802594367764572825570801015673920656423356258608441 1139 / 1221458158822048512299116262767 07

5559847073041673800279150748892523203286958159479142299341203951560045538721686217 7

Fourth Example

Moral: don't make your primes out of powers at all if they're going to end up very different in size.

Actually, you know what: forget the whole powers thing.

Fifth Example

n=22297505287621151926579523443756494443560284637980895301079051218492663150409699661436423510035299346156823095761317493687768386518189303297622101044813472505 99

This one looks pretty good.

The $\sqrt{n+r^2}$ trick doesn't work.

No integer base produces any sequences of zeros, so it's not been made using powers.

Fifth Example

n=22297505287621151926579523443756494443560284637980895301079051218492663150409699661436423510035299346156823095761317493687768386518189303297622101044813472505 99

In fact, the primes were found using a pretty secure technique.

By this guy.

Fifth Example

Moral: they give lecturers access to the Internet too these days.

How to beat me

Choose two large **random** integers and find primes slightly greater (or less) than them both.

That's it.

I'll *literally* never crack it in a million years.