maths careers
endless opportunities

more maths grads
multiplying opportunities

what's the point of...

PRIME NUMBERS?

Maths makes the world go round

Every time money is moved over the internet, whether it's multi-million pound transactions or payments of less than a pound, prime numbers are used to make sure that the money is moved securely.

When data, such as your bank card details, is sent over the internet it needs to be sent in code, or encrypted, so that if it was intercepted by criminals they wouldn't be able to use it. Encrypting data uses a 'key'. Early methods used the same key to both encrypt and decrypt messages. The problem with sending data over the internet is that the key for encrypting data needs to be freely available so that anyone can send in a transaction (this is known as the 'public key') but the key for undoing the code needs to be secret so that if criminals intercept the message they can't decrypt it (this is known as the 'private key').

It is very difficult to find a system where you can't easily find the private key if you know the public one. In the 1970s, however, three American mathematicians, Ron Rivest, Adi Shamir and Leonard Adleman developed a method based on prime numbers. This method has been named RSA after them.

RSA uses the idea that multiplying two large prime numbers together is relatively easy but factorising them is much more difficult.

The public key uses the product of two large prime numbers and the private key uses the two prime numbers separately. If you think it sounds easy, try to find which two 8-digit prime numbers have been multiplied together to give

1 427 462 380 339 871.

Secure systems over the internet use prime numbers with a hundred digits or more!

If you use a bank card to buy something from a website your card details are encrypted and sent over the internet. If someone intercepts this encrypted message it will be meaningless – only the bank, with its knowledge of the private key, will be able to decrypt and find out your card number. This security isn't just restricted to financial transactions, for example a similar method can also be used when sending emails: you can digitally 'sign' emails to prove they came from you.

In the early part of the 20th century the mathematician G H Hardy worked on prime numbers. He was fiercely proud of being a Pure Mathematician and famously stated "Nothing I have ever done is of the slightest practical use". Prime numbers are now at the heart of countless secure transactions every day!

Maths is useful in my book!

Books have a unique number on them to identify them. Before 2005 a 10-digit number was used, known as the International Standard Book Number (ISBN).

The first nine numbers identify the book and the last is a check digit. The last digit is generated by multiplying the first digit by 10, the second by 9 and so on, then adding up all the results. The remainder when this is divided by 11 is subtracted from 11 to give the check digit. (The remainder could be 10, in which case an X is used, or the number may be exactly divisible by 11, in which case a 0 is used.)

For example 0951611208 is a 10-digit ISBN number.
$0 \times 10 + 9 \times 9 + 5 \times 8 + 1 \times 7 + 6 \times 6 + 1 \times 5 + 1 \times 4 + 2 \times 3 + 0 \times 2 = 179$
This gives a remainder of 3 when divided by 11.
$11 - 3 = 8$ so it is likely that the ISBN number is correct.

Because 11 is a prime number it doesn't have any factors in common with the multipliers (10, 9, ..., 2). If a mistake has been made by copying down a number incorrectly or confusing the order of two of the numbers then the check digit will be incorrect.

Since 2005 13-digit ISBNs have been used but finding a suitable number, large enough to not have factors in common with the multipliers and with enough symbols (the X is no longer used) has been difficult and the check digit in 13-digit ISBNs do not show up all possible errors generated by either getting a single number wrong or copying down two numbers in the wrong order.

Maths is, like, totally random

Random numbers are very useful in many situations. Random numbers can be generated by physical objects like rolling dice but this is very time consuming and in many situations it is useful to be able to generate random numbers on a computer.

For example many computer games use random number generators to simulate 'real life' so that the opposition players in your football game aren't too predictable or so the baddies don't always come at you at the same time in a shoot out. The lotteries in some countries also use random-number generators to choose the numbers.

Random numbers are also very important in simulations. Modelling the weather, the spread of diseases or the number of people using the queues in a supermarket all involve random events. Mathematical modellers need to generate random numbers to create computer-based simulations so they can try different strategies for dealing with events.

Generating truly random numbers on a computer is impossible but mathematicians have created functions that appear as if they are random. These are known as pseudo-random number generators and prime numbers feature heavily in these functions.

• For further information, articles and resources visit: www.moremathsgrads.org.uk • www.mathscareers.org.uk plus.maths.org • nrich.maths.org • www.cs4fn.org

• Written by Tom Button, Peter McOwan, Matt Parker and Zia Rahman
• Special thanks to Professor David Arrowsmith (QMUL), Makhan Singh, Melanie Ashfield and James Anthony, University of Birmingham

Mixed Sources
Product group from well-managed forests and other controlled sources
www.fsc.org Cert no. QA COC-837950
© 1996 Forest Stewardship Council

Design: info@jamesanthonygraphics.com Reorder: info@pinstripegroup.co.uk - quote 41813