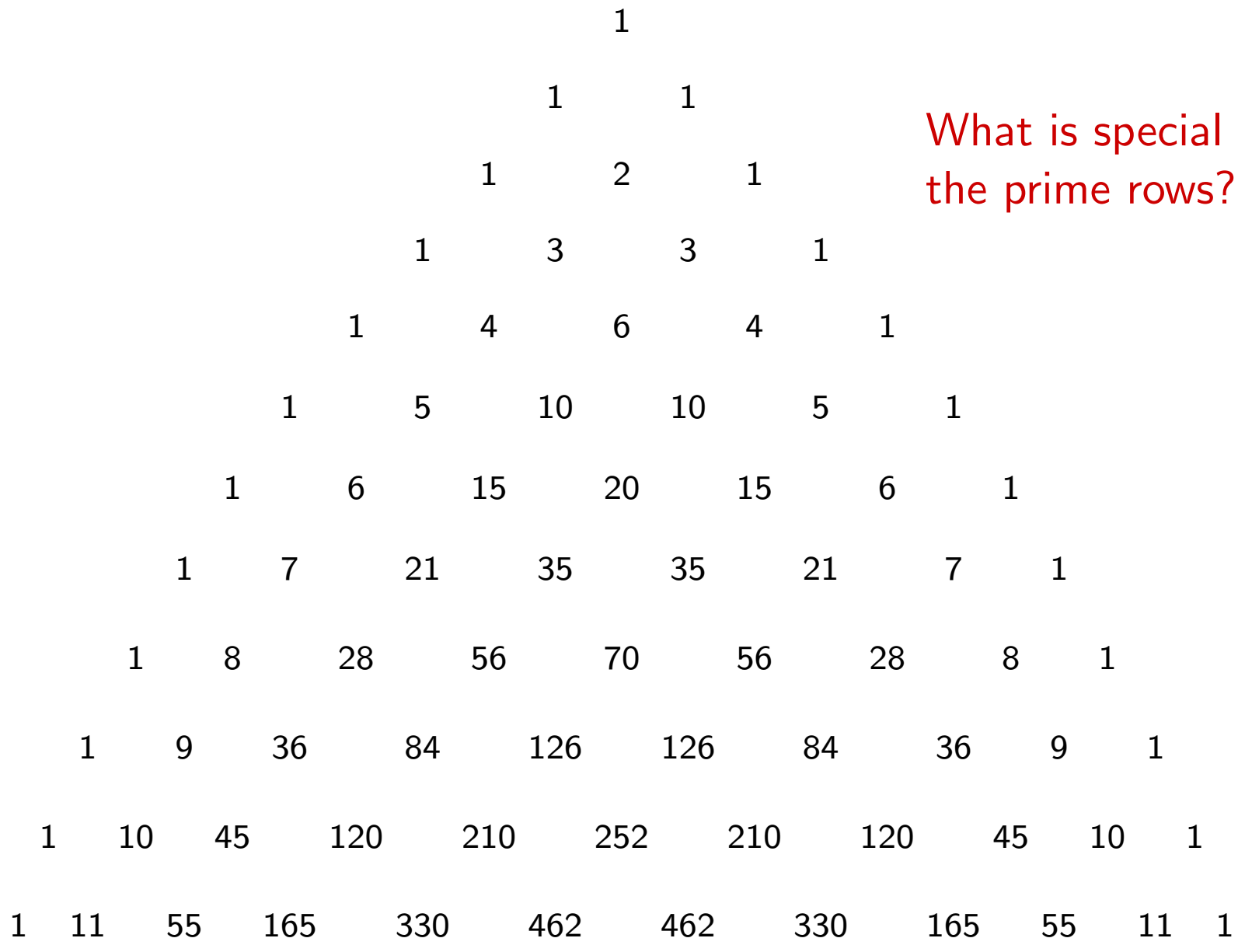
Open key encryption after Rivest-Shamir-Adleman

A contribution to the MUMS student seminar series

by Nora Ganter, University of Melbourne.

Prime Rows in the Pascal Triangle



What is special about the prime rows?

Divisibility of prime rows

The pth row in the Pascal triangle lists the numbers

$$\binom{p}{k} = \frac{p \times (p-1) \times \cdots \times (p-k+1)}{k \times (k-1) \times \cdots \times 1}$$

The simplified fraction is a natural number, namely the number of possibilities to choose k objects out of a set of p.

The number p divides the numerator but not the denominator. If p is a prime number, it follows that it divides $\binom{p}{k}$, too.

Here we assumed $1 \leq k \leq p-1$ and used, without proof:

Euler's Lemma: If a prime number p divides a product, then it divides at least one of the factors.

Fermat's little theorem

Fix a prime p and let a be a natural number. Then

$$a^p \equiv a \mod p,$$

i.e., the remainders of a^p and a when dividing by p are equal.

Proof by induction, starting at $a = 0$.

Multiplication modulo p

Let a be an integer, and let p be a prime number.

Multiplication with a modulo p is a one-to-one correspondence:

$$\begin{array}{rcl} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & a \\ 2 & \longleftrightarrow & 2 \times a \\ & \vdots & \\ p-1 & \longleftrightarrow & (p-1) \times a. \end{array}$$

Proof: Euler's Lemma.

Multiplicative inverses modulo p

If p is understood, we write $a^{-}1$ for any natural number with

$$a \times a^{-1} \equiv 1 \equiv a^{-1} \times a \qquad \text{mod } p.$$

This characterises a^{-1} uniquely modulo p. Modulo p, multiplication with a^{-1} is inverse to multiplication with a.

Example: What is the inverse of 3 modulo 7?

This property makes the set $\{[0], [1], \ldots [p-1]\}$ of remainder classes, endowed with addtion and multiplication modulo p, a field, known as $\mathbb{F}_p$ to mathematicians, $GF(p)$ to computer scientists.

Reformulation of Fermat's little theorem

Using the existence of multiplicative inverses in $\mathbb{F}_p$, we can rewrite Fermat's little theorem as follows:

Either p divides a and all its powers or

$$a^{p-1} \equiv 1 \mod p.$$

Extended Euclidean algorithm

Algorithmically, our existence proof is not practicable.

Instead, use the extended Euclidean algorithm for determining the greatest common divisor. This yields a constructive proof of a stronger result:

Bezout's Lemma says that given a and n, there exist b and k such that

$$ab + kn = \gcd(a, n).$$

Example: $n = 7$ and $a = 3$.

Basics of RSA encryption

Secret: p and q, two large prime numbers.

Public: the product $n = pq$, to be used as modulus.

Secret: the product $(p-1)(q-1)$.

Public: the encryption key e, which is chosen to be coprime to $(p-1)(q-1)$.

Secret: the decryption key $d = e^{-1}$ modulo $(p-1)(q-1)$.

To encrypt a message m, form the eth power $c = m^e$ modulo n. Then send the encrypted message c.

The receipient decodes the message by taking the dth power of c,

$$c^d \equiv m \mod n.$$

Why does it work?

Theorem:

$$(c^d) = m^{ed} \equiv m \qquad \text{mod } n.$$

Proof: We need to show that

$$p \text{ divides } m^{ed} - m \qquad \text{and} \qquad q \text{ divides } m^{ed} - m.$$

By Bezout's Lemma there exists $k \in \mathbb{N}$ such that

$$ed = 1 + k(p-1)(q-1)$$

Hence

$$\begin{aligned} m^{ed} &\equiv \left(m^{k(q-1)}\right)^{p-1} \times m \\ &\equiv m \end{aligned}$$

by Fermat's little theorem.