UPPSALA UNIVERSITET

Summary of *Primes is in P*[*]

Christopher Kjellqvist

* Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. In Annals of Mathematics, 160, pages 781–791, 2004.

Primality

- A number n is prime if no number in [2..n-1] divides n
- Greek philosopher Eratosthenes has a prime sieve attributed to his name
- Other Properties:
  - Fermat's Little Theorem: for any a, a^{p-1} mod p
  - $(X + a)^n = (X^n + a) \bmod n$ iff n is prime

https://commons.wikimedia.org/wiki/File:Eratosthene.01.png

UPPSALA UNIVERSITET

Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

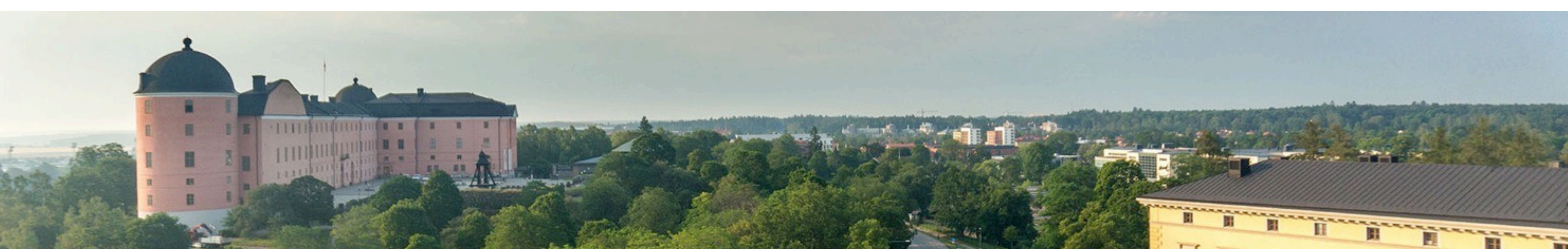
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

UPPSALA UNIVERSITET

Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

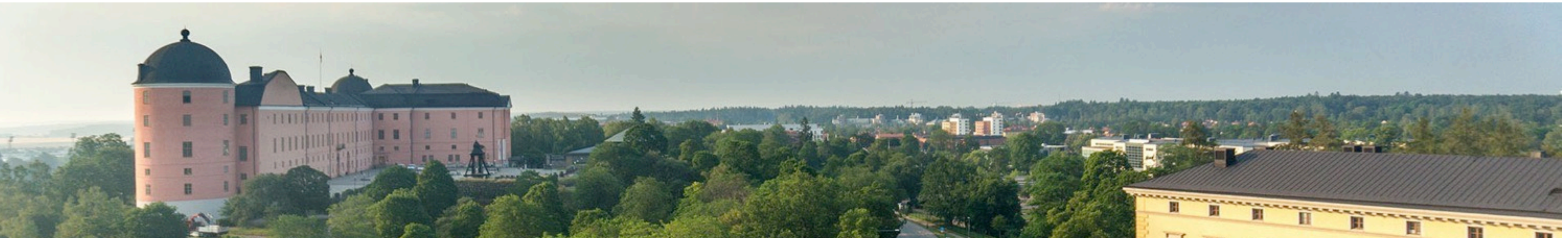
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

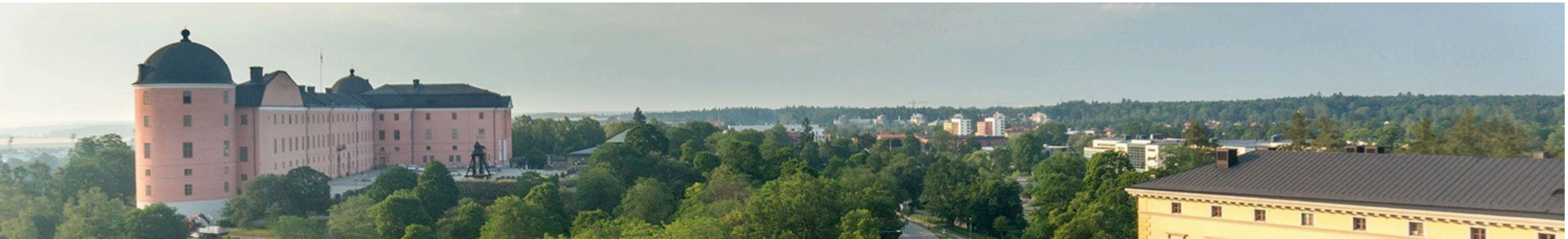
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

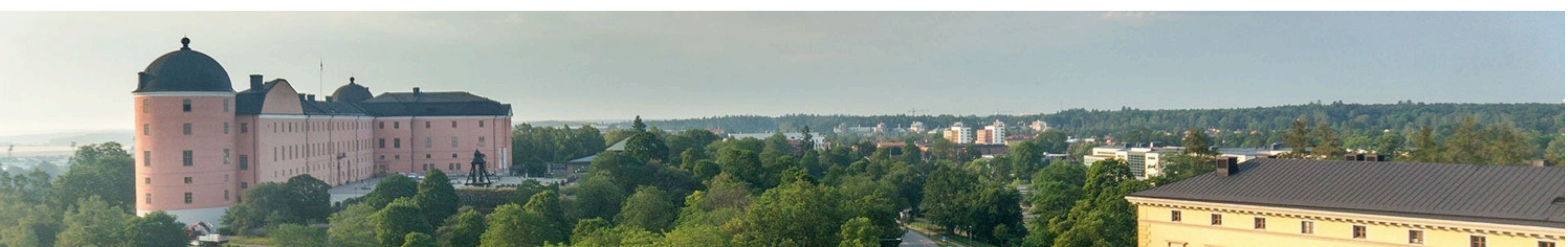
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

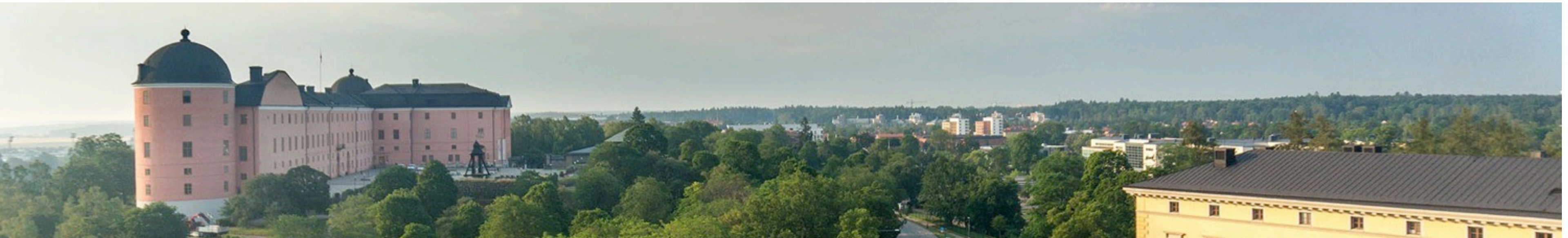
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

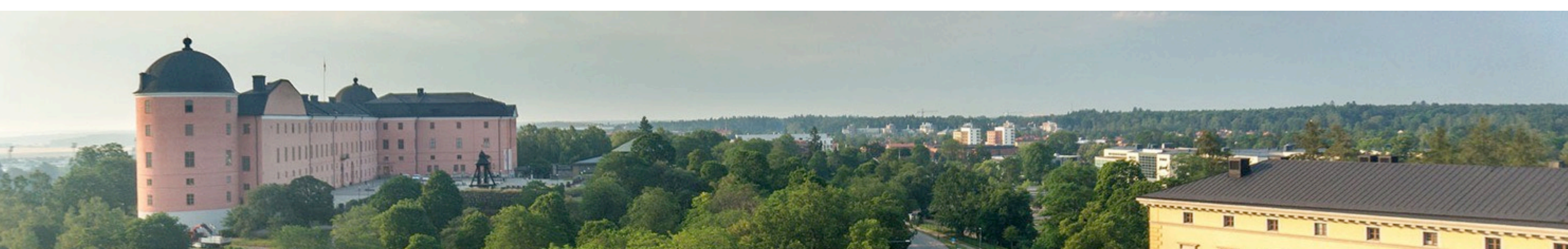
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

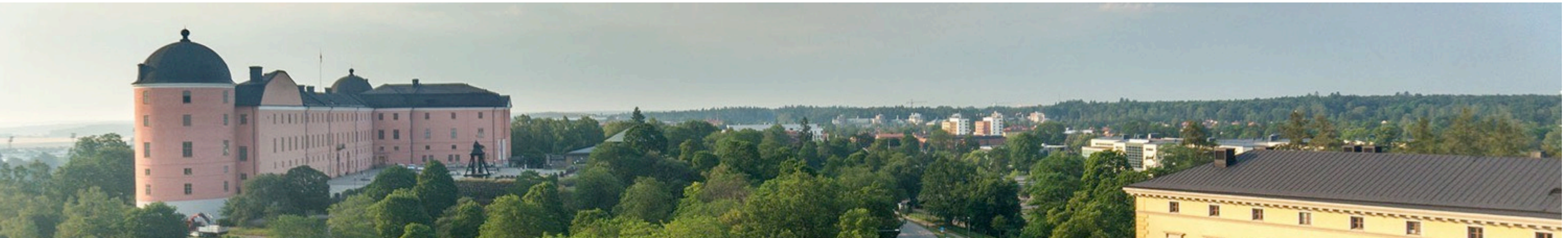
1	2	3	4	5	6	7	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100



Sieve of Eratosthenes

- Find all the primes < *n*
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



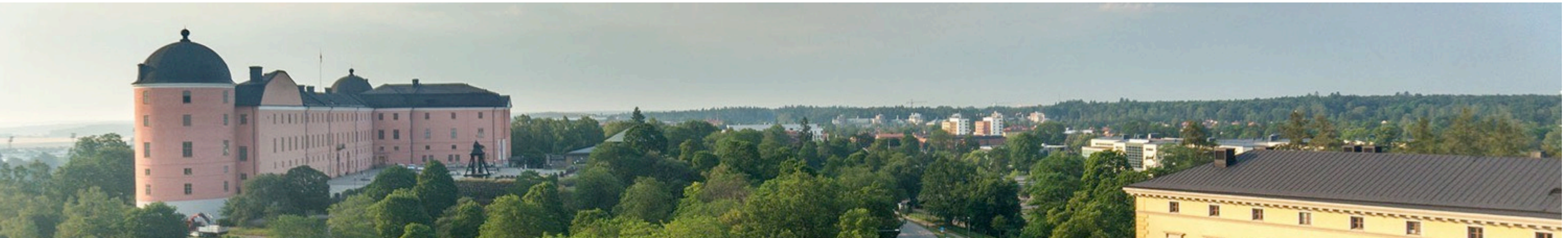
UPPSALA UNIVERSITET

Sieve of Eratosthenes

- Find all the primes < n
- Find the first unmarked number and mark it as prime
- For all of its multiples, mark them as composite
- Time Complexity:

  $\mathcal{O}(n \log \log(n))$
- Density of primes related to $\log \log(n)$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



Fermat's Little Theorem

$$\forall a \in \mathbb{N} \,|\, a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

UPPSALA UNIVERSITET

Fermat's Little Theorem

$\forall a \in \mathbb{N} \,|\, a \neq p, a^{p-1} \equiv 1 \mod p$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

561

UPPSALA UNIVERSITET

Fermat's Little Theorem

$$\forall a \in \mathbb{N} \,|\, a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

561

$$2^{560} \equiv 1 \mod 561$$

Fermat's Little Theorem

$$\forall a \in \mathbb{N} \mid a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

561

$$2^{560} \equiv 1 \mod 561$$
$$5^{560} \equiv 1 \mod 561$$

UPPSALA UNIVERSITET

Fermat’s Little Theorem

$$\forall a \in \mathbb{N} \mid a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

$$561$$

$$2^{560} \equiv 1 \mod 561$$
$$5^{560} \equiv 1 \mod 561$$
$$23^{560} \equiv 1 \mod 561$$

UPPSALA UNIVERSITET

Fermat's Little Theorem

$$\forall a \in \mathbb{N} \mid a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

561

$$2^{560} \equiv 1 \mod 561$$
$$5^{560} \equiv 1 \mod 561$$
$$23^{560} \equiv 1 \mod 561$$
$$100^{560} \equiv 1 \mod 561$$

Fermat's Little Theorem

$$\forall a \in \mathbb{N} \,|\, a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm

$$561 = 3 \cdot 11 \cdot 17$$

$$2^{560} \equiv 1 \mod 561$$
$$5^{560} \equiv 1 \mod 561$$
$$23^{560} \equiv 1 \mod 561$$
$$100^{560} \equiv 1 \mod 561$$

UPPSALA UNIVERSITET

Fermat’s Little Theorem

$$\forall a \in \mathbb{N} \,|\, a \neq p, a^{p-1} \equiv 1 \mod p$$

- Potentially the key to a $\mathcal{O}(poly(\log n))$ algorithm
- Carmichael Numbers

$$561 = 3 \cdot 11 \cdot 17$$

$$2^{560} \equiv 1 \mod 561$$
$$5^{560} \equiv 1 \mod 561$$
$$23^{560} \equiv 1 \mod 561$$
$$100^{560} \equiv 1 \mod 561$$

- Hard to find except by finding factorization…
- Still is a good way of finding ‘probable’ primes

Primes is in P

$$(X + a)^p \equiv X^p + a \mod p$$

Primes is in P

$$(X + a)^p \equiv X^p + a \mod p$$

- In a polynomial $(x+y)^n$, the coefficient of the i’th term will be $\binom{n}{i}$
- As long as n is prime, that coefficient will be divisible by *n*
- The first and last terms will cancel out

Primes is in P

$$(X + a)^p \equiv X^p + a \mod p$$

- In a polynomial $(x + y)^n$, the coefficient of the i'th term will be $\binom{n}{i}$
- As long as n is prime, that coefficient will be divisible by *n*
- The first and last terms will cancel out

$$(X + a)^p - X^p - a \equiv 0 \mod p$$

UPPSALA UNIVERSITET

Primes is in P

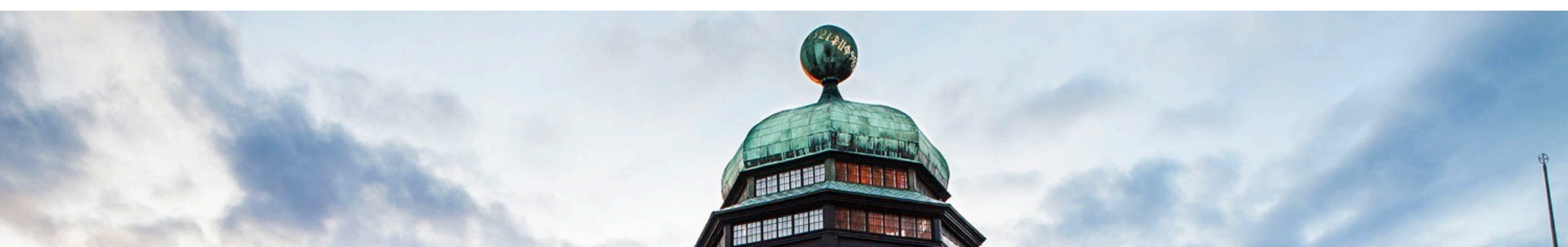
$$(X+a)^p \equiv X^p + a \mod p$$

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad \boxed{2} \quad 1 \\
1 \quad \boxed{3 \quad 3} \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad \boxed{5 \quad 10 \quad 10 \quad 5} \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad \boxed{7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7} \quad 1 \\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
1 \quad 9 \quad 36 \quad 84 \quad 126 \quad 126 \quad 84 \quad 36 \quad 9 \quad 1 \\
1 \quad 10 \quad 45 \quad 120 \quad 210 \quad 252 \quad 210 \quad 120 \quad 45 \quad 10 \quad 1
\end{array}
$$

Primes is in P

Input: Integer $n > 1$

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output **COMPOSITE**



Primes is in P

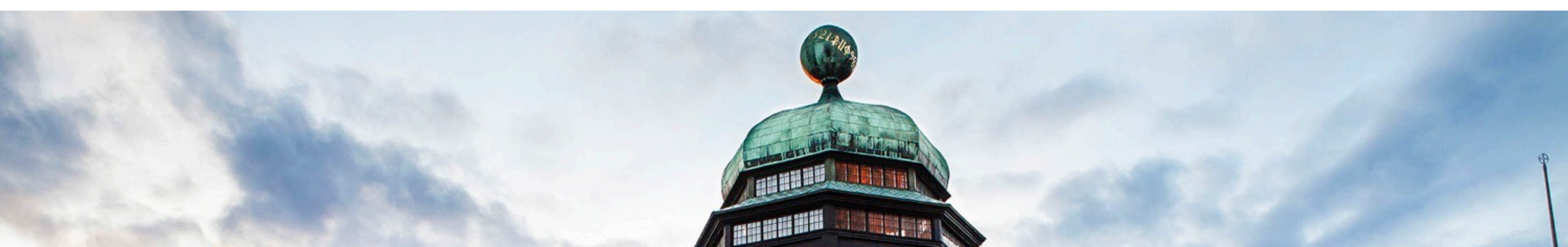
Input: Integer $n > 1$

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output **COMPOSITE**
2. Find the smallest r such that $o_r(n) > \log^2 n$.

- The order of a modulo is the smallest k such that

$$n^k \equiv 1 \mod r$$

$$7^{10} \equiv 1 \mod 11 \quad o_{11}(7) = 10$$

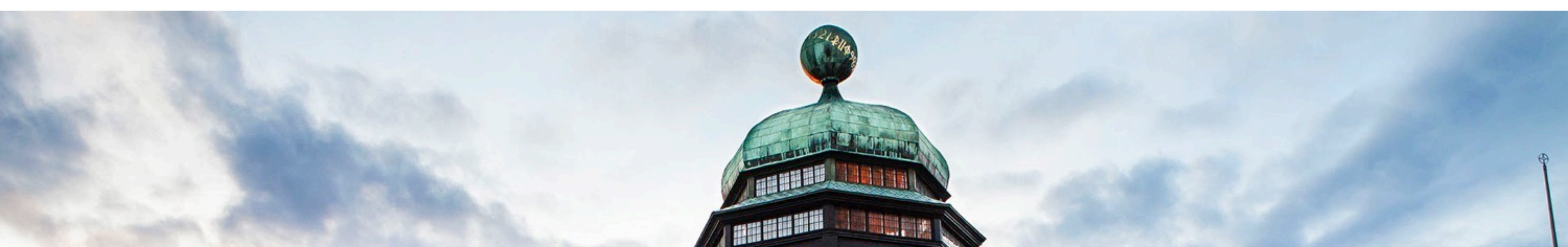


UPPSALA
UNIVERSITET

Primes is in P

Input: Integer $n > 1$

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output **COMPOSITE**
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output **COMPOSITE**



Primes is in P

Input: Integer $n > 1$

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output **COMPOSITE**
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output **COMPOSITE**
4. If $n \leq r$ output **PRIME**

- If n is less than r and we found the LCM of every number in [2..r], then n must have no prime divisors

ϕ: Euler's Totient Function

- $\phi(n)$ is equal to the number of numbers less than *n* that are relatively prime to *n*

$$
\begin{aligned}
\phi(6) &= 2 \quad \{1,5\} \\
\phi(7) &= 6 \quad \{1,2,3,4,5,6\} \\
\phi(8) &= 4 \quad \{1,3,5,7\}
\end{aligned}
$$

Primes is in P

Input: Integer $n > 1$

1. If ($n = a^b$ for $a \in \mathbb{N}$ and $b > 1$), output **COMPOSITE**
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output **COMPOSITE**
4. If $n \leq r$ output **PRIME**

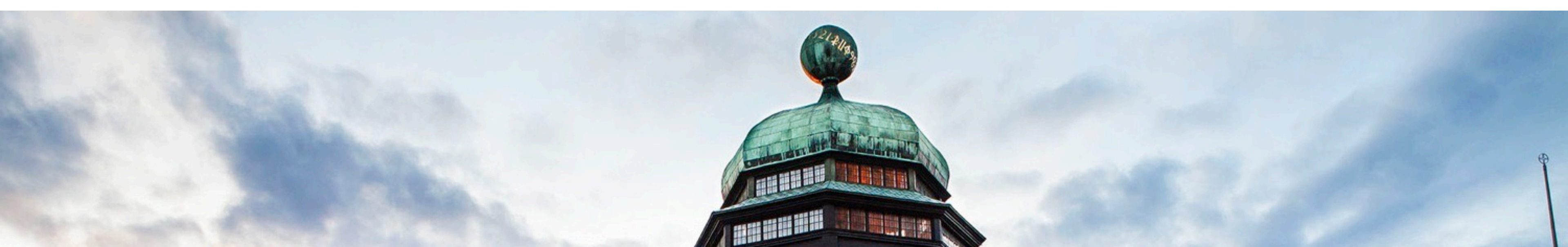
for $a = 1$ *to* $\lfloor \sqrt{\phi(r)} \log n \rfloor$ **do**

  5. if $((X + a)^n \neq X^n + a(\mod X^r - 1, n))$, output **COMPOSITE**

end

6. Output **PRIME**

- The term $\lfloor \sqrt{\phi(r)} \log n \rfloor$ is what gives this algorithm its deterministic polynomial time complexity



Conclusion

- Prior sieves come with undesirable qualities
  - Exponential Growth
  - Edge cases
- *Primes is in P* gives us a deterministic polynomial time algorithm with no edge cases