Hledání rekordně velkých prvočísel

Martina Bekrová
Ondřej Bouchala
David Krška
Lukáš Vacek

17. června 2010

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Eratosthenovo síto

Definice

Prvočíslo je takové přirozené číslo p, které má právě dva dělitele. (1 a p)

	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

Marin Mersenne (1588-1648)

- Matematik (teorie čísel)
- Teolog
- Hudební teoretik (”Otec akustiky”)
- Duchovní otec Akademie věd

Mersennova čísla

Definice

Mersennovo číslo je každé přirozené číslo, které můžeme zapsat ve tvaru:

$$M_p := 2^p - 1$$

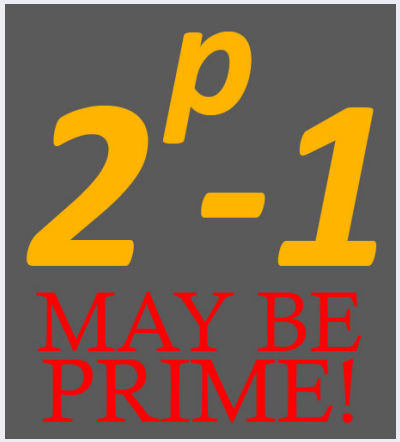
Pokud je toto číslo prvočíslem, pak se nazývá Mersennovým prvočíslem.

$$2^{mn} - 1 = (2^m - 1)\left(1 + 2^m + 2^{2m} + \ldots + 2^{(n-1)m}\right)$$

Mersenne: p =2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

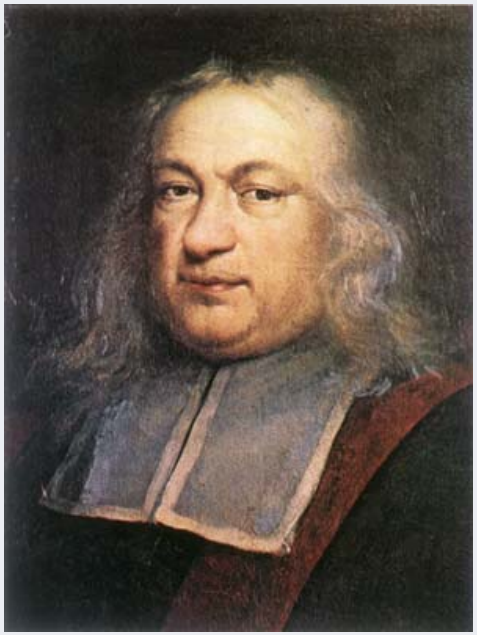
Skutečnost: p =2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127

GIMPS – Great Internet Mersenne Prime Search



- Propojení počítačů přes internet
- 13 z 47 nalezených
- Největší: $2^{43\,112\,609} - 1$ (12 978 189 cifer)
- EFF – odměny za nalezení prvočísel (150 000/250 000 USD)
- http://www.mersenne.org/

Fermatova čísla



Obrázek: Pierre de Fermat (1601 - 1665)

Definice

Fermatovo číslo je takové číslo, pro které platí:

$$F_m = 2^{2^m} + 1, \textit{ kde } m \textit{ je přirozené číslo.}$$

Fermatova čísla

- Fermat byl přesvědčen, že všechna Fermatova čísla jsou prvočísla
- Prvních 5 Fermatových čísel jsou prvočísla:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537$$

- Dále je známo, že F_5 až F_{32} jsou složená
- Nevyřešený problém je, zda je Fermatových prvočísel nekonečně mnoho

Druhy testů

- Přesné testy
- Pravděpodobnostní testy

Lucas-Lehmerův test

- Testuje pouze Mersennova prvočísla
- Definujeme posloupnost $y_1 = 4,\ y_{k+1} = y_k^2 - 2$
- Mersennovo číslo $M_p = 2^p - 1$ je prvočíslo právě tehdy, když M_p dělí y_{p-1}
- Tento algoritmus je rychlejší než všechny ostatní testy

Pozn.

Pomocí tohoto testu Lucas objevil největší prvočíslo M_{127} bez použití počítače

Pépinův test

- Testuje pouze Fermatova prvočísla
- Fermatovo číslo $F_m = 2^{2^m} + 1$ je prvočíslo právě tehdy, když $3^{\frac{F_m - 1}{2}} \equiv -1 \mod F_m$

Pozn.

Pépin toto tvrzení dokázal v roce 1877 pro základ 5, zjednodušení si všiml Lucas

Miller-Rabinův test

- Použijeme vztah $p - 1 = 2^s d$, kde p je prvočíslo a d číslo liché
- Dále si zvolíme přirozené číslo a, které je menší než p
- Pak musí platit:
  - Buď $a^d \equiv 1 \mod p$,
  - nebo $a^{2^r d} \equiv -1 \mod p$ pro nějaké $0 \leq r \leq s - 1$.

Pozn.

Pravděpodobnost, že pro p složené test n-krát neodhalí neprvočíselnost p, je $1/4^n$.

Děkujeme za pozornost