Seminár z algoritmizácie a programovania 1

Martin Bobák
Ústav informatiky
Slovenská akadémia vied

Obsah prednášky

1. **Prvočísla**

Spätná väzba:
https://forms.gle/iKbuLdF6xDtNSEDP8

Prvočísla

Prvočísla

Definícia: Prvočíslo je prirodzené číslo, ktoré je väčšie ako 1, a ktorého jedinými deliteľmi (v množine prirodzených čísiel) sú 1 a ono samé.

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, …
- nekonečne veľa
- špeciálnym prípadom prvočísiel sú tzv. Mersennove prvočísla, ktoré sa dajú zapísať v tvare $n = 2^p - 1$, kde p je taktiež prvočíslo.

Ostatné čísla, vznikajú (je ich možné rozložiť) ako súčiny viacerých prvočísiel, a nazývajú sa **zložené čísla**.

- Výnimku tvoria čísla 0 a 1, ktoré nie sú prvočísla, pričom ich neoznačujeme ani ako zložené čísla.
- Každé prirodzené číslo väčšie než 1, je možné jednoznačne rozložiť na súčin prvočísiel jediným spôsobom (pri ich zoradení podľa veľkosti)
  napr. : 78 = 2 * 3 * 13 153 = 3 * 3 * 17

Testovanie prvočísiel

- najjednoduchším riešením je testovanie deliteľnosti čísla n, postupne číslami i = 2, 3, 4, 5, 6, 7, ... floor(sqrt(n)).
  - operátor MODULO (v jazyku C je reprezentovaný symbolom %), vyjadrujúci zvyšok po celočíselnom delení.
  - ak je splnená podmienka **if (n % i == 0)**, potom dané číslo rozhodne nemôže byť prvočíslo. Cyklus s premennou i teda môže byť prerušený, a ďalšie testovanie deliteľnosti čísla n nie je potrebné.
  - naopak, v prípade ak táto podmienka nie je splnená, napr. pre i = 3, ešte to neznamená že n je to prvočíslo. Je nutné testovať deliteľnosť až po i = floor(sqrt(n)).
  - Až po prejdení celého tohto rozsahu, v prípade ak žiadny zvyšok nie je rovný 0, môžeme s určitosťou tvrdiť, že dané číslo je prvočíslo.
  - Časová náročnosť/zložitosť takéhoto prístupu je O(n/2) = **O(n)**.

Testovanie prvočísiel
Rekurzívne

```
int isPrime(int n, int i)
{
  if (n < 2)
    return 0;
  if (n < 4)
    return 1;
  if ((n%i == 0) && (i > 1))
    return 0;
  if (i < 2)
    return 1;
  return isPrime(n, i-1);
}
```

Testovanie prvočísiel

- pravdepodobnostné metódy.
  - tieto metódy sú výrazne rýchlejšie, obzvlášť pre vysoké čisla, avšak ich nevýhodou je, že nedávajú vždy správny výsledok (je však vysoká pravdepodobnosť, že je výsledok správny).
  - vychádzajú z teórie čísiel, numerickej matematiky ako aj rôznych pokročilejších štatistických vlastností prvočísiel.

Hromadné vyhľadávanie prvočísiel

- vyhľadávať všetky prvočísla od 2 do stanovenej hranice, je výrazne efektívnejšie použitie algoritmu - určitého typu sita na hľadanie prvočísiel (sieve for prime numbers).
  - Najznámejšie sú 3 takéto algoritmy (Eratostenovo sito, Atkinovo sito, Sundaramovo sito).
- najrozšírenejším je Eratostenovo sito
  - testované čísla sú spracovávané hromadne
  - algoritmus je možné implementovať bez použitia operácie násobenia, delenia a modula (iba s jedným použítím odmocniny, aj to mimo cyklu)
  - časová zložitosť algoritmu: O(n.log(log(n)))

Eratostenovo sito

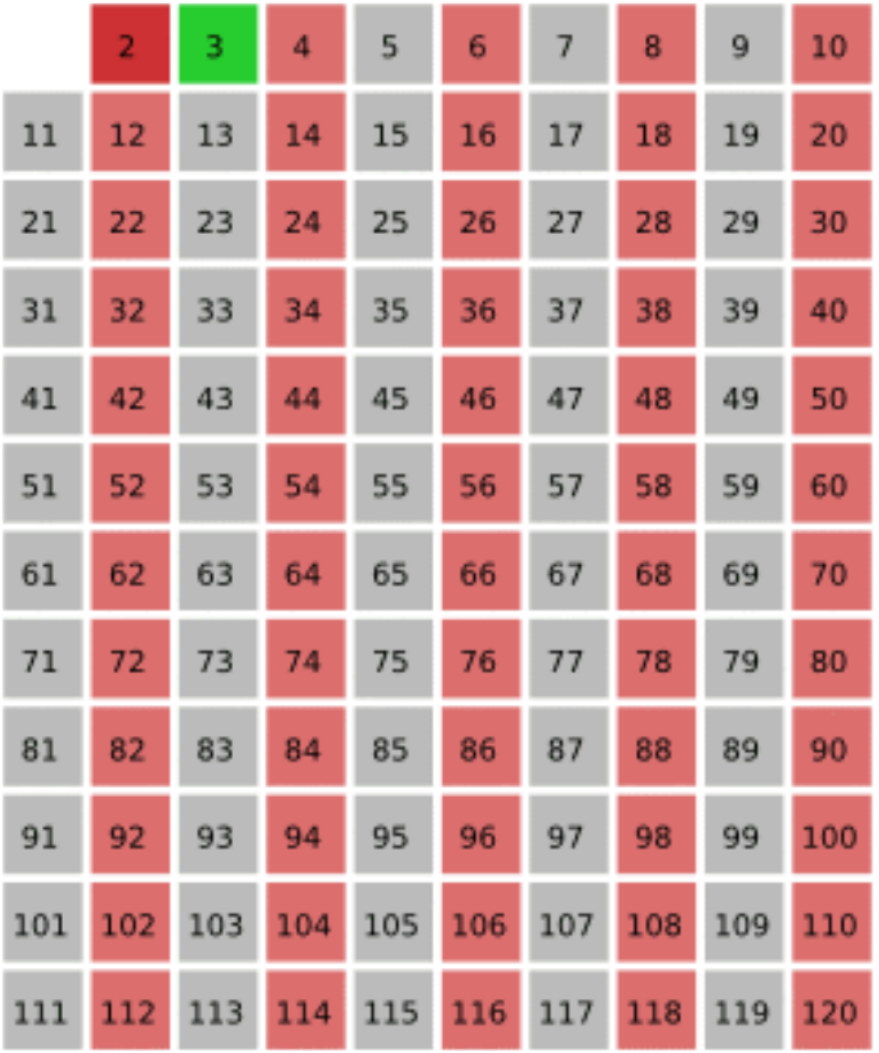
1. Zoznam obsahuje všetky čísla v rozsahu 2 po N
2. Odoberieme prvé číslo zo zoznamu a označíme ho ako prvočíslo
3. Odoberieme zo zoznamu všetky násobky práve odobratého prvočísla
4. Pokračujeme opäť bodom 2, pokiaľ ostávajú nejaké čísla
   - stačí ísť po floor (sqrt (N))

Eratostenovo sito

	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Eratostenovo sito

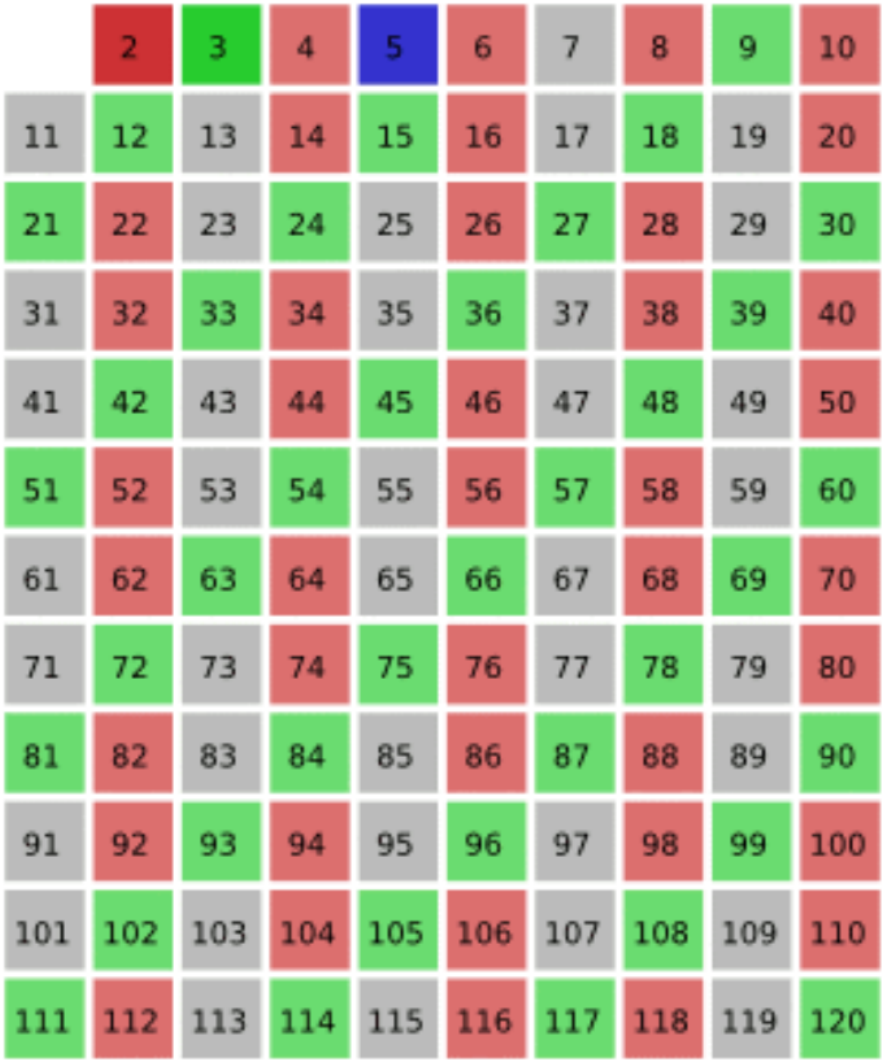


	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

2 3

Eratostenovo sito



Eratostenovo sito

Eratostenovo sito

Prime numbers

2 3 5 7

11

Eratostenovo sito

	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

2	3	5	7
11	13	17	19
23	29	31	37
41	43	47	53
59	61	67	71
73	79	83	89
97	101	103	107
109	113		

Zdroje

[1] en.wikipedia.org

Ďakujem vám za pozornosť!

Spätná väzba:
https://forms.gle/iKbuLdF6xDtNSEDP8