《CSP-J 初级组算法中数学》

Day03-初等数论(下)

主讲人：小武老师

可达信奥_小武老师_keda.ac

课程大纲

1️⃣初等数论 (上)
奇数、偶数、质数、合数、约数、倍数、因数、最小公倍数、最大公约数、欧几里得算法等

2️⃣初等数论 (中)
算术基本定理、同余关系、孙子定理等

3️⃣初等数论 (下)
质数判定、质数筛、埃氏筛法、线性筛法等

4️⃣函数 (上)
坐标、函数图像、一次函数、变量与函数等

5️⃣函数 (下)
二次函数、指数函数、对数函数、根式与指数幂、幂运算等

6️⃣数列基础
等差数列、等比数列、递推公式、通项公式等

7️⃣矩阵基础
一维矩阵、二维矩阵、矩阵的运算、转置、杨辉三角等

8️⃣数及其运算
数的进制、二进制、八进制、十六进制、编码（ASCII）等

9️⃣计数原理与排列组合 (上)
加法原理、乘法原理、排列与组合、再看杨辉三角等

🔟计数原理与排列组合 (下)
捆绑法、插空法、CSP真题训练等

同余练习

同余关系、习题选讲

同余

定义1： 如果a和b都是整数而m是一个固定的正整数，则当m|(a-b)(即m能够整除a-b)时，我们就说a,b对模m同余，记作：

$$a \equiv b(\mathrm{mod} m)$$

当m不能整数a-b时，则我们就说a,b对模m不同余，记作：

$$a \not\equiv b(\mathrm{mod} m)$$

$29 \equiv 2(\mathrm{mod}9)$

$93 \equiv -7(\mathrm{mod}50)$

$161 \not\equiv 0(\mathrm{mod}8)$

$257 \equiv 16(\mathrm{mod}32)$

同余

判断以下式子是否正确（即是否同余）

$29 \equiv 2 (\mathrm{mod} 9)$ （ √ ）

$29 \div 9 = 3 \cdots 2$

$2 \div 9 = 0 \cdots 2$

$9 | (29 - 2)$

9能整除27 $9 | 27$

$161 \not\equiv 0 (\mathrm{mod} 8)$ （ √ ）

$161 \div 8 = 20 \cdots 1$

$0 \div 8 = 0 \cdots 0$

$8 \nmid 161$

8不能整除161

同余

判断以下式子是否正确（即是否同余）

如果有两个整数a,b，其中b>0，如果a=bq+r，q,r都是整数，且0≤r<b

```
-7=50*(?)+r
 a=bq+r
```

$93 \not\equiv -7 (\mathrm{mod} 50)$ （×）

$93 \div 50 = 1 \cdots 43$

$-7 \div 50 = -1 \cdots 43$

$50 | (93 - (-7))$

50能整除100 $50 | 100$

同余

例1 今天是星期一，再过100天是星期几？ 答案：星期三

$$100 \div 7 = 14 \cdots 2$$

例2 如果98和66除以同一个数都余2，求这个数是多少？ 答案：4、8、16、32

$$98 \div x = q_1 \cdots 2$$

$$66 \div x = q_2 \cdots 2$$

$$\Rightarrow 98 \equiv 66 (\bmod x) \Rightarrow x | (98 - 66) \Rightarrow x | 32$$

x能整除32

32 的约数有：1、2、4、8、16、32 ⇒ 除数要大于余数 ⇒ 4、8、16、32

同余

例3　如果82,98和66除以同一个数都余2，求这个数是多少？　答案：4、8、16

$$\begin{cases} 82 \div x = q_1 \cdots 2 \\ 98 \div x = q_2 \cdots 2 \\ 66 \div x = q_3 \cdots 2 \end{cases} \rightarrow \begin{cases} 80 \div x = q_1 \cdots 0 \\ 96 \div x = q_2 \cdots 0 \\ 64 \div x = q_3 \cdots 0 \end{cases} \rightarrow x \mid (80, 96, 64)$$

$$(80, 96, 64) = ? \rightarrow \begin{cases} 80 = 2^4 \times 5 \\ 96 = 2^5 \times 3 \\ 64 = 2^6 \end{cases} \rightarrow (80, 96, 64) = 2^4 = 16$$

16 的约数有：1、2、4、8、16 → 除数要大于余数 → 4、8、16

同余

例4 如果101和80除以同一个大于1的数，余数相同，求这个数是多少？ 答案：3、7、21

$101 \equiv 80 (\mathrm{mod} x)$ → $x|(101-80)$ → $x|21$

x能整除21

21 的约数有：1、3、7、21 → 除数要大于余数 → 3、7、21

同余

例5　如果87,52和31除以A（A>1）的余数相同，求A是多少？　答案：7

$$87 \equiv 52 \equiv 31 (\mathrm{mod}\, A) \rightarrow \begin{matrix} A|(87-52) \\ A|(87-31) \\ A|(52-31) \end{matrix} \rightarrow \begin{matrix} A|35 \\ A|56 \\ A|21 \end{matrix} \rightarrow A|(35,56,21)$$

$$(35,56,21) = ? \rightarrow \begin{matrix} 35 = 5 \times 7 \\ 56 = 2^3 \times 7 \\ 21 = 3 \times 7 \end{matrix} \rightarrow (35,56,21) = 7$$

同余

例6 如果141和239除以同一个大于1的数，余数分别为a和a+18，求这个数是多少？

答案：20、40、80

$$141 \equiv 221 (\mathrm{mod}\, x) \quad \rightarrow \quad x|80$$

80 的约数有：1、2、4、5、8、10、16、20、40、80 → 20、40、80

验证，因为有可能a+18大于除数（比如151和249就无解）

20、40、80 → 20、40、80

同余

和的余数 = 余数的和

$$(139+235)\div 9$$

$$139\div 9\cdots 4$$

$$235\div 9\cdots 1$$

$$(4+1)\div 9\cdots 5$$

积的余数 = 余数的积

$$(139\times 235)\div 9$$

$$139\div 9\cdots 4$$

$$235\div 9\cdots 1$$

$$(139\times 235)\div 9\cdots 4$$

$$(123\times 235+233\times 875)\div 9$$

$$123\div 9\cdots 6$$

$$233\div 9\cdots 8$$

$$235\div 9\cdots 1$$

$$875\div 9\cdots 2$$

$$(6\times 1+8\times 2)\div 9\cdots 4$$

质数筛

质数判定、埃氏筛法、线性筛法

质数与合数

定义2： 一个大于1的正整数，只能被1和它本身整除，不能被其它正整除整除，这样的正整数叫做素数（也叫做质数）。

eg. $2, 3, 5, 7, 11, 13, 17, 19$ 都是质数

Q3: 如何判定一个数是质数?

定义3： 一个正整数除了能被1和它本身整除以外，还能被另外的正整数整除，这样的正整数叫做复合数（也叫做合数）。

eg. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20$ 都是合数

Q4: 如何判定一个数是合数?

开根号法判定质数

引理2：如果a是一个大于1的整数，而所有≤√a的素数都除不尽a，则a是素数。

Step 1：证明（1）：如果a被 > 1 而 ≤ √a的整数都除不尽，则a是素数

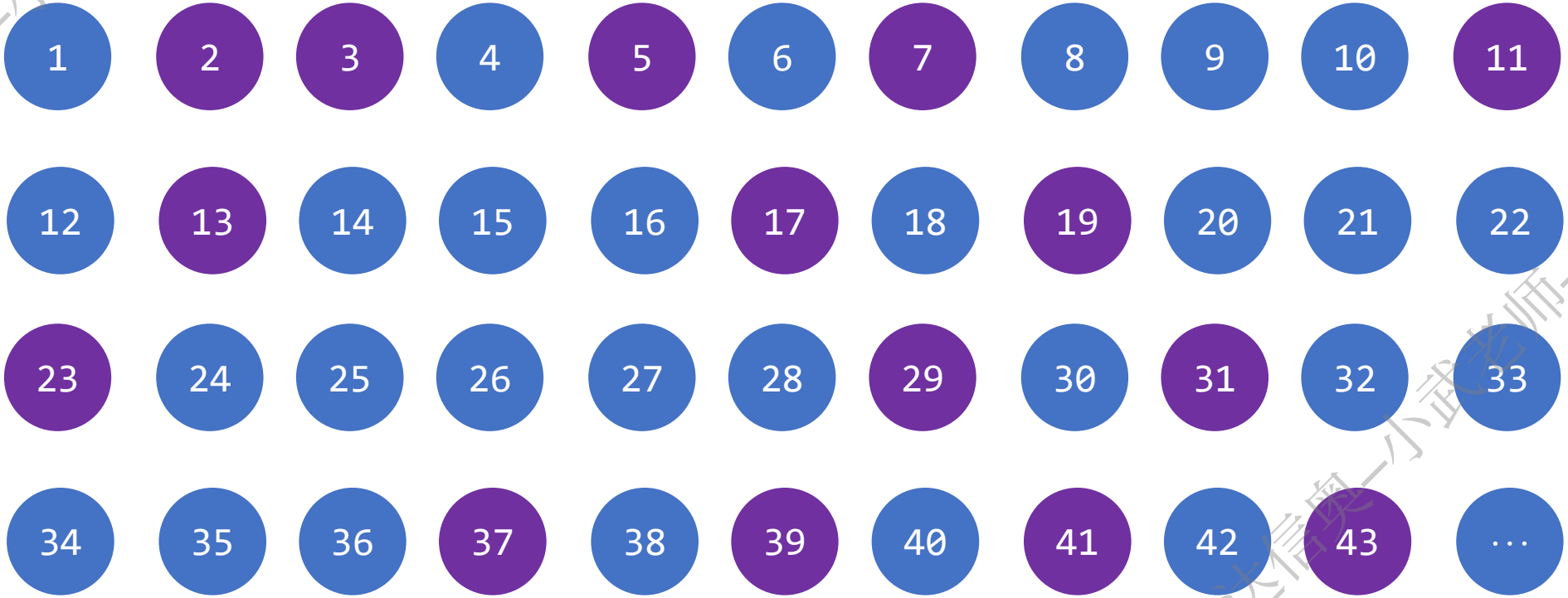
假设a是合数，则 a=bc，而a被> 1 而 ≤ √a的整数都除不尽，则 b> √a，c> √a,则bc>a,这与 bc=a 是矛盾的。

```
bool isPrime(int n){
    if (n == 0 || n == 1) return false;
    for (int i = 2; i <= sqrt(n); i++){
            if( n%i == 0){
                return false;
            }
        }
    return true;
}
```

开根号法判定质数

质数筛

质数筛（素数筛）：给定一个整数，求出之间的所有质数(素数)，这样的问题为质数筛(素数的筛选问题)。



埃氏筛法

埃拉托斯特尼 Eratosthenes
（前276年－前194年）

古希腊数学家、诗人、天文学家

埃拉托斯特尼筛法

测量地球周长

埃氏筛法

基本思想：任意整数x的倍数$2x,3x,\ldots\ldots$都不是质数

↓ 算术基本定理

任意质数x的倍数$2x,3x,\ldots\ldots$都不是质数

埃氏筛法

Step 1：首先将0、1排除；

Step 2：创建从2到n的连续整数列表，[2,3,4,…,n]；

Step 3：初始化 p = 2，因为2是最小的质数；

Step 4:：枚举所有p的倍数(2p,3p,4p,…)，标记为非质数（合数）；

Step 5：找到下一个没有标记且大于p的数。如果没有，结束运算；如果有，将该值赋予p，重复步骤4；

Step 6：运算结束后，剩下所有未标记的数都是找到的质数。

	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

埃氏筛法

Step 1：首先将0、1排除；

Step 2：创建从2到n的连续整数列表，[2,3,4,…,n]；Step 3：初始化 p = 2，因为2是最小的质数；

Step 4:：枚举所有p的倍数(2p,3p,4p,…)，标记为非质数（合数）；

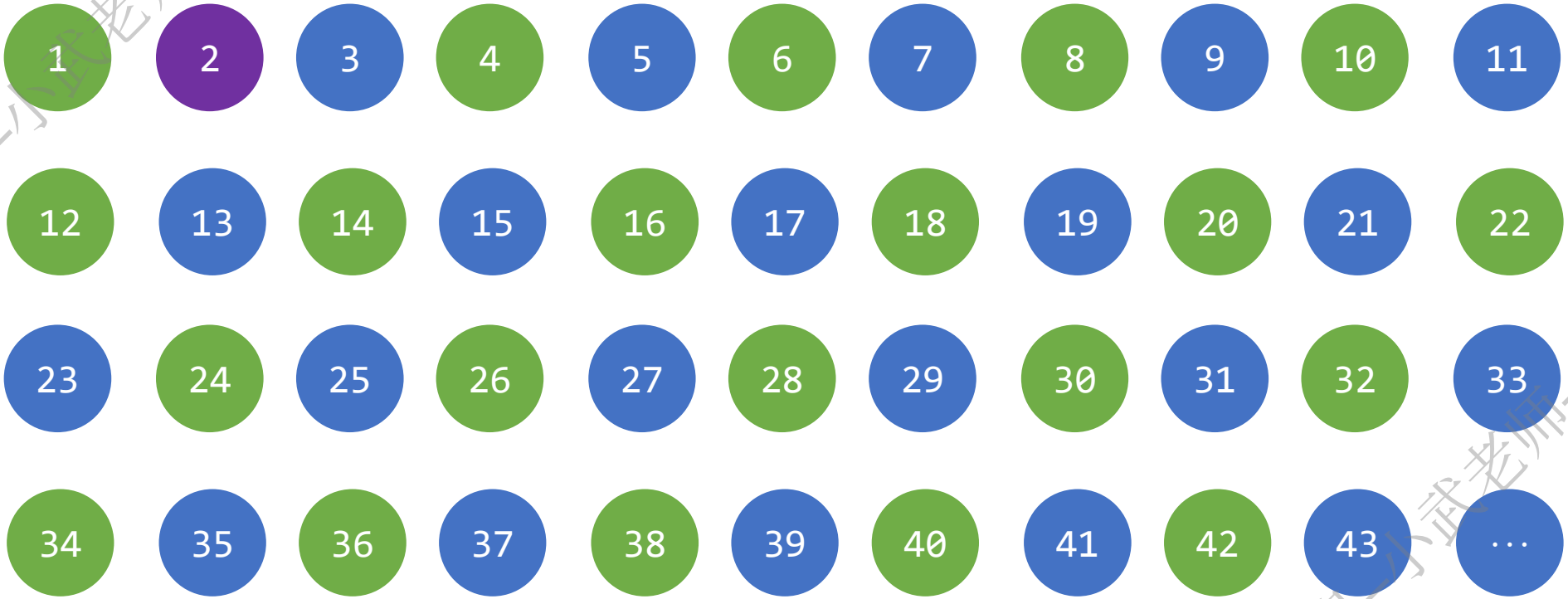
Step 5：找到下一个没有标记且大于p的数。如果没有，结束运算；如果有，将该值赋予p，重复步骤4；

Step 6：运算结束后，剩下所有未标记的数都是找到的质数。

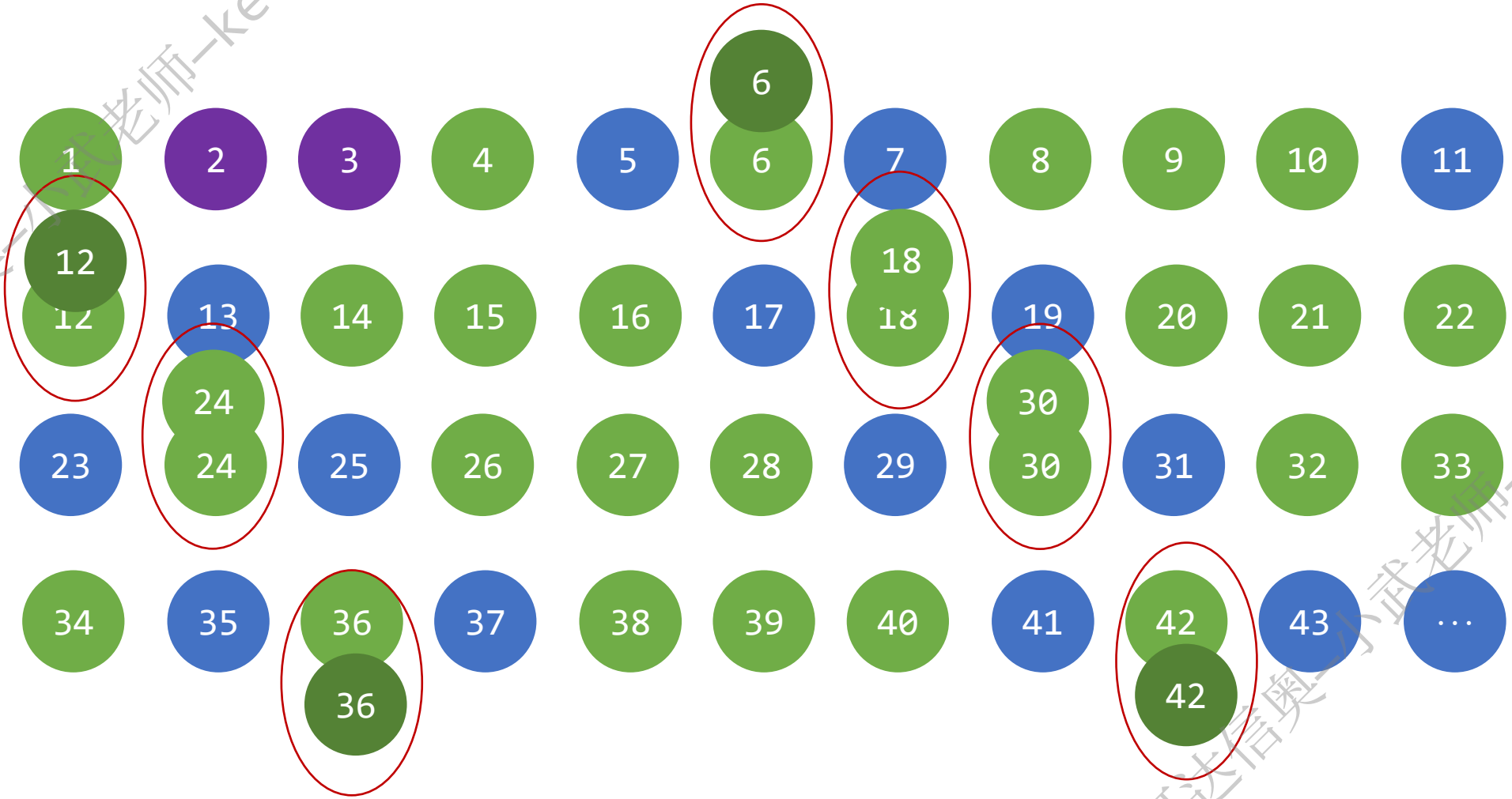
```
int Eratosthenes(int n){
    for(int i = 1;i <= n; i++) is_p[i]=1;
    memset(prime,0,sizeof(prime));
    is_p[1] = is_p[0] = 0;
    for(int i = 1;i <= n;i++){
        if(!is_p[i]) continue;
        prime[++tot]=i;//prime[]存储了[1,n]的所有质数
        for(int j = i*2; j <= n; j+=i) is_p[j]=0;//j
为合数
    }
    return tot;
}
```

埃氏筛法

埃氏筛法有什么优化的空间?



埃氏筛法



线性筛法

埃氏筛会重复标记已标记的合数。例如12会被质数2重复标记，同时也会被2标记。

根本原因：没有唯一的产生12的乘积的方式

仅能标记一次合数就好了

算术基本定理

每个合数只会被它的最小质因子筛一次

$12 = 2 \times 2 \times 3$

$35 = 5 \times 7$

线性筛（欧拉筛）

线性筛法

欧拉筛法的基本思想：在埃氏筛法的基础上，让每个合数只被它的最小质因子筛选一次，以达到不重复的目的。

欧拉（1707-1783）

瑞士数学家、自然科学家

13岁时入读巴塞尔大学“**所有人的老师**”

数学史上最多产的数学家

各种欧拉公式

最小质因子筛选 = 最大非自身因数

$4 = 2 \times 2$

$6 = 2 \times 3$

$9 = 3 \times 3$

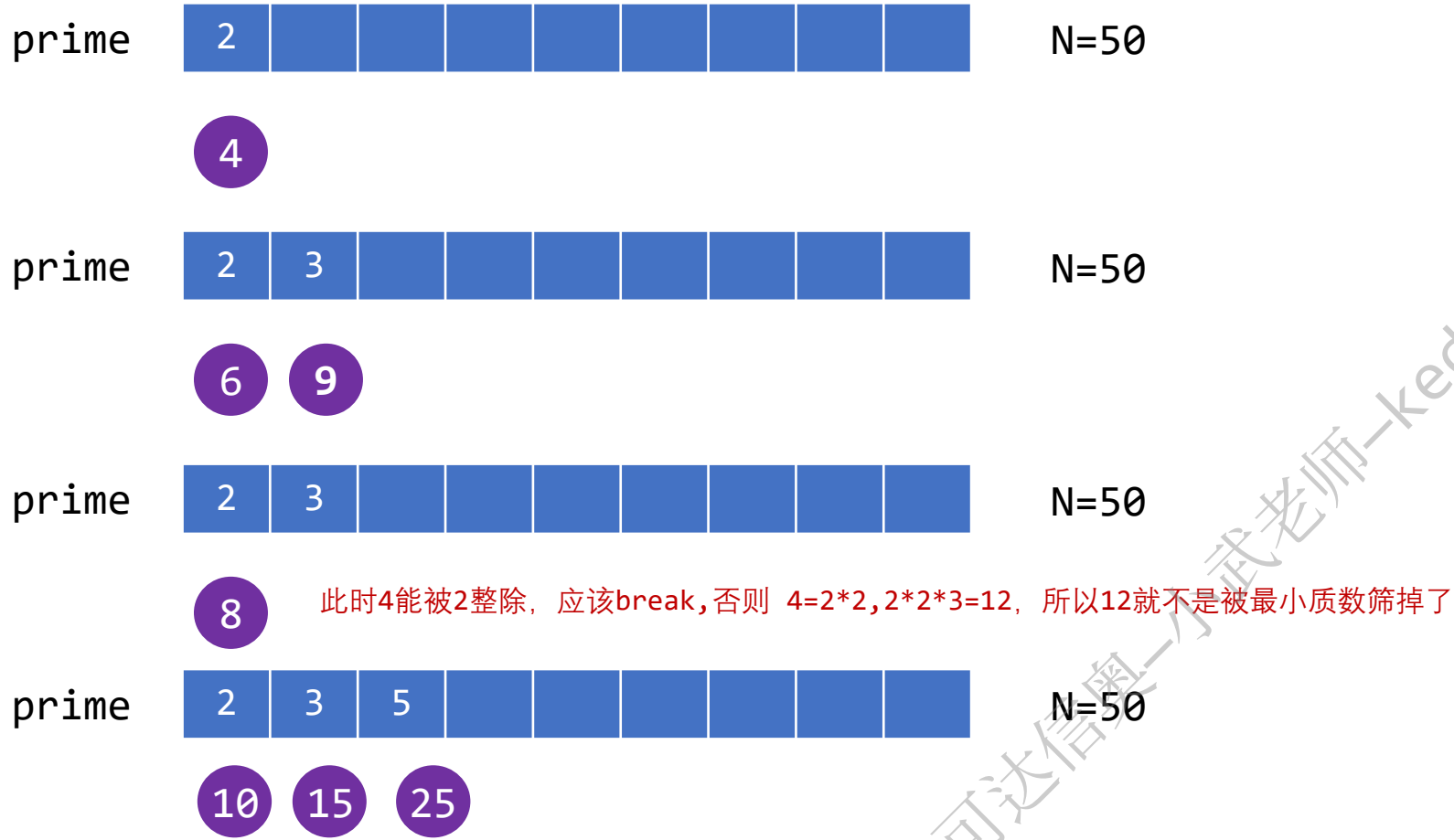
$8 = 2 \times 2 \times 2$

$10 = 2 \times 5$

$35 = 5 \times 7$

线性筛法

欧拉筛法的基本思想：在埃氏筛法的基础上，让每个合数只被它的最小质因子筛选一次，以达到不重复的目的。



线性筛法

i 的值	质数表[数组]	筛去的数?
2	2	
3	2,3	
4	2,3	
5	2,3,5	
6	2,3,5	
7	2,3,5,7	
8	2,3,5,7	
9	2,3,5,7	

筛去的数
4
6,9
8
10,15,25
12
14,21,35,49
16
18,27

线性筛法

欧拉筛法的基本思想：在埃氏筛法的基础上，让每个合数只被它的最小质因子筛选一次，以达到不重复的目的。

欧拉（1707-1783）
瑞士数学家、自然科学家
13岁时入读巴塞尔大学“**所有人的老师**”
数学史上最多产的数学家
各种欧拉公式

Step 1 依次枚举每一个数

Step 2 若当前数没被筛，则把这个数加入质数集合

Step 3 对于每一个数，枚举当前已知质数，并相应筛掉当前数 × 枚举到的质数 .而被筛掉的那个数的最小质因数一定是枚举到的质数。

Step 4 如果i 是枚举到的质数的倍数，停止枚举质数

线性筛法

欧拉筛法的基本思想：在埃氏筛法的基础上，让每个合数只被它的最小质因子筛选一次，以达到不重复的目的。

```
if(i%prime[j] == 0) break
```

这段程序保证了筛掉的那个数的最小质因数一定是prime[j]

```
memset(is_prime, 1, sizeof(is_prime)); //1
    is_prime[0] = is_prime[1] = 0;
    for(int i = 2; i <= n; i++){
        if(is_prime[i]){
            prime[cnt++] = i;    //加入到质数数组里
        }
        for(int j = 1; j < cnt && prime[j]*i <= n; j++){  //关键一
            is_prime[prime[j]*i] = 0;
            if(i%prime[j] == 0) break;// 关键二
        }
    }
```

i的最小质因子是prime[j]

如果到j后不break，那么继续筛下去会不用最小质因数筛数，是无用的

因为每个合数只会被它的最小质因子筛一次，所以线性筛的复杂度为O(n)。

初等数论总结

1 初等数论 (上)
奇数、偶数、质数、合数、约数、倍数、因数、最小公倍数、最大公约数、欧几里得算法等

2 初等数论 (中)
算术基本定理、同余关系、孙子定理等

3 初等数论 (下)
质数判定、质数筛、埃氏筛法、线性筛法等

4 函数 (上)
坐标、函数图像、一次函数、变量与函数等

5 函数 (下)
二次函数、指数函数、对数函数、根式与指数幂、幂运算等

6 数列基础
等差数列、等比数列、递推公式、通项公式等

7 矩阵基础
一维矩阵、二维矩阵、矩阵的运算、转置、杨辉三角等

8 数及其运算
数的进制、二进制、八进制、十六进制、编码（ASCII）等

9 计数原理与排列组合 (上)
加法原理、乘法原理、排列与组合、再看杨辉三角等

10 计数原理与排列组合 (下)
捆绑法、插空法、CSP真题训练等

课后习题与实验

Talk is cheap, show me the code !

下节课见啦！