Information Security

Information
信息安全 Security
系列丛书

信息安全数学基础

许春香　周俊辉　编著

电子科技大学出版社

Information
信息安全Security
系列丛书

信息安全数学基础

许春香　周俊辉　编著

电子科技大学出版社

图书在版编目（CIP）数据

信息安全数学基础/许春香，周俊辉编著. —成都：电子科技大学出版社，2008.3

信息安全系列丛书

ISBN 978-7-81114-520-5

Ⅰ.信… Ⅱ.①许… ②周… Ⅲ.信息系统—安全技术—应用数学—高等学校—教材 Ⅳ.TP309 029

中国版本图书馆 CIP 数据核字（2008）第 017035 号

内 容 提 要

本书为信息安全系列丛书之一，系统地介绍了信息安全技术所必需的数学基础知识，包括近世代数和初等数论。本书对这两部分内容进行了融合，使之成为一个有机的整体。

本书可作为信息安全专业、计算机专业、通信专业本科生、研究生教材，还可以供信息安全技术领域科技人员参考。

信息安全系列丛书

信息安全数学基础

许春香 周俊辉 编著

出 版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）
策划编辑：曾 艺
责任编辑：曾 艺
主 页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发 行：新华书店经销
印 刷：成都蜀通印务有限责任公司
成品尺寸：185mm×260mm 印张 9 字数 220 千字
版 次：2008 年 3 月第一版
印 次：2008 年 3 月第一次印刷
书 号：ISBN 978-7-81114-520-5
定 价：18.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

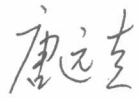
秦志光　李建平　周明天

序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。



二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

前言

信息安全技术的核心是密码学，信息安全数学基础是学习密码学所必需的数学基础知识，包括近世代数和初等数论。由于信息安全技术在现代社会的快速发展和广泛应用，信息安全数学基础也得到了普遍重视。

信息安全数学基础包含的都是抽象的数学内容，它概念多，结论（定理）多，而且概念一般都没有物理意义，这对习惯微积分等物理意义明确的数学课程的工科读者来说是一个挑战。我们编写本书时只选取最基本、最必需的内容，力图使用简单清晰的语言，使之尽量符合工科数学课程的风格。我们认为，只要反复研习，再抽象的内容也能变得具体起来，变得容易把握。

近世代数与初等数论本来是两门课程，以前只为数学专业开设，一般是在学习近世代数之前学习数论，把数论作为学习近世代数的基础课程。信息安全数学基础把它们融合成一门课程，这就存在它们能不能够融合和怎么融合两个问题。近世代数与初等数论是相关性很强的两门课程，例如，整除与同余既是数论的开端，也是近世代数的先导预备知识。再如，某些结论（费马定理等）既可由近世代数导出，也可由数论导出，因此这两门课程的融合是可能的，而且融合也是它们共同作为信息安全技术数学基础的客观需要。因为对于信息安全技术领域的读者来说，分别完整学习近世代数和初等数论两门课程内容显得过多，耗时耗力，没有必要，而在一门课程里同时包含近世代数和初等数论中的必要内容，既满足要求，又高效实用。

如何融合近世代数和初等数论？我们有两种选择：第一，按传统的思路，先引入数论，再引入近世代数，在了解剩余类、剩余系、原根等概念的基础上学习近世代数的群、环、域。第二，先引入近世代数，再引入数论，先建立群、环、域的框架，再在此基础上学习数论，尽量将数论的内容纳入群、环、域的框架中。这两种选择各有其合理之处。数论先于近世代数发展起来，因此前者符合其自然发展过程。数论的很好掌握也有助于近世代数的学习。而后者的融合性好，将两部分内容汇合成一个整体，很好地克服了前者数论和代数“两张皮”的不足。此外，第一个选择在数论部分结束时开始近世代数部分，代数部分概念多且抽象，内容已经过半，而与之前联系不紧密的新概念突然如潮涌来，这很不符合一般学习习惯。数论部分概念相对少一些，而且易于理解，因此放在后面更有利于读者学习。需要指出的是，当把近世代数和初等数论作为独立课程学习时，初等数论作为先导课程学习要更为合理一些。

我们在编写本书的过程中采取的是第二种选择，即先建立群、环、域的框架，再引入数论。在数论部分，我们尽量将群、环、域的结论应用到数论之中。例如，由群的结论直接得到欧拉定理等，但为了使读者从多个角度更好地理解，我们同时也给出了数论的直接描述。实际上本书只是我们在讲授信息安全数学基础课程经验基础上的一个尝试，如何编写出符合

信息安全技术发展需求的信息安全数学基础教材仍然是一个值得探讨的课题。

建议读者在通过本书学习信息安全数学基础时把握好以同余为基石的脉络：同余——剩余类（群）——剩余类环——剩余系（特别是简化剩余系）——同余式，这条脉络尽管不能认为是本书的主线，但可以串起本书的大部分核心内容，把握好它对于从总体上掌握好该门课程非常有帮助。

本书可作为信息安全专业本科生、研究生教材，还可以供信息安全技术领域科研人员参考。

笔者衷心感谢我国著名的密码学专家肖国镇教授，是他把笔者带入密码学领域，笔者今天才能够进行本书的编写工作。同时衷心感谢郝玉洁老师和曾艺老师，没有她们的大力推动，本书不可能呈现在读者面前。最后衷心感谢电子科技大学计算机学院领导和同事们在信息安全数学基础教学和本书编写中给予的支持和帮助。

许春香　周俊辉

2008.1

目录

第 1 章　整除与同余

第 2 章　群

第 3 章　循环群、群的结构

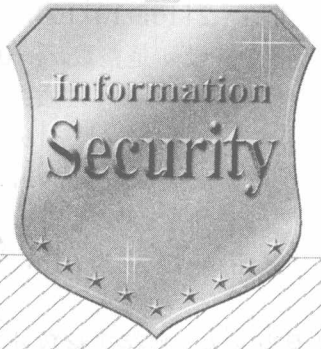
第 4 章　环

第 5 章　多项式环与有限域

第 6 章　同余式

第 7 章 平方剩余

第 8 章 原根与离散对数



第1章

整除与同余

整除和同余是学习后面章节的基础. 整除、素数等概念在初等数学中就曾经涉及，但我们这里要进行更加系统和深入的讨论.

1.1 整除

定义 1 设 a，b 是任意两个整数，其中 $b\neq 0$，如果存在一个整数 q，使 $a=qb$，则我们称 b 整除 a，或 a 被 b **整除**，记为 $b|a$，此时称 b 是 a 的**因子**，a 是 b 的**倍数**.

例 1 $2|10$，$10|100$.

例 2 设 a 是整数，$a\neq 0$，则 $a|0$.

整除有下列基本性质：

（1）如果 $b|a$ 且 $a|b$，则 $b=a$ 或 $b=-a$.

（2）如果 $a|b$ 且 $b|c$，则 $a|c$.

（3）如果 $c|a$ 且 $c|b$，则 $c|ua+vb$，其中 u，v 是整数.

证明：（1）因为 $b|a$，则存在整数 q_1，使

$$a=q_1b.$$

又因为 $a|b$，则存在整数 q_2，使

$$b=q_2a.$$

于是

$$a=q_1b=q_2q_1a.$$

所以我们有 $q_2q_1=1$，由于 q_1，q_2 是整数，则

$$q_2=q_1=1，\text{或 } q_2=q_1=-1.$$

故

$$b=a \text{ 或 } b=-a.$$

（2）因为 $a|b$，则存在整数 q_1，使

$$b=q_1a.$$

又因为 $b|c$，则存在整数 q_2，使

$$c=q_2b.$$

于是

$c=q_2b=q_1q_2a=qa$，其中 $q=q_1q_2$.

故 $a|c$.

（3）仿照（1）、（2）的证明很容易证得.

当两个整数不能整除时，我们有**带余除法：**

对于 a，b 两个整数，其中 $b\neq 0$，则

$$a=bq+r，\ 0\leqslant r<|b|.$$

r 称为 a 被 b 除得到的**余数**. 显然当 $r=0$ 时，$b|a$.

例 3（1）$a=-37$，$b=5$，则

$$-37=(-8)\times 5+3，\ r=3.$$

（2）$a=41$，$b=-5$，则

$$41=(-8)\times(-5)+1,\ r=1.$$

定义 2 （1）设 a，b 是两个整数，如果整数 $c\mid a$ 且 $c\mid b$，则 c 称为 a，b 的**公因子**.

（2）设 $c>0$ 是两个不全为零的整数 a，b 的公因子，如果 a，b 的任何公因子都整除 c，则 c 称为 a，b 的**最大公因子**，记为 $c=(a,\ b)$.

由最大公因子的定义立即有：

$$(a,\ b)=(-a,\ b)=(a,\ -b)=(-a,\ -b),$$
$$(0,\ a)=|a|.$$

例 4 2，5，10 是 20，30 的公因子. 20，30 的最大公因子$(20,\ 30)=10$.

求最大公因子的一般方法是使用下面的**欧几里得除法**（又称**辗转相除法**）.

设 a，b 是两个正整数，记 $r_0=a$，$r_1=b$，于是我们有：

$$r_0=q_1r_1+r_2,\ 0\leqslant r_2<r_1,$$
$$r_1=q_2r_2+r_3,\ 0\leqslant r_3<r_2,$$
$$\cdots$$
$$r_{n-2}=q_{n-1}r_{n-1}+r_n,\ 0\leqslant r_n<r_{n-1},$$
$$r_{n-1}=q_nr_n.$$
$$r_n=(a,\ b)$$

欧几里得除法的原理如下：

由上述除法过程可看出，r_n 整除 r_{n-1}，r_{n-2}，…，r_2，r_1，r_0，所以 r_n 是 a，b 的公因子.

如果 d 是 a，b 的任意公因子，从上面除法的第一行向下可以看出，d 整除 r_0，r_1，则 d 整除 r_2，r_3，…，r_{n-2}，r_{n-1}，r_n. 故 r_n 是最大公因子，$r_n=(a,\ b)$.

例 5 （1）$a=888$，$b=312$，求$(a,\ b)$.

（2）$a=-3824$，$b=1837$，求$(a,\ b)$.

解：①

$$\underline{888}=2\times\underline{312}+\underline{264}$$
$$\underline{312}=1\times\underline{264}+\underline{48}$$
$$\underline{264}=5\times\underline{48}+\underline{24}$$
$$\underline{48}=2\times\underline{24}$$

故$(888,\ 312)=24$.

②

$(-3824,\ 1837)=(3824,\ 1837)$.

$$\underline{3824}=2\times\underline{1837}+\underline{150}$$
$$\underline{1837}=12\times\underline{150}+\underline{37}$$
$$\underline{150}=4\times\underline{37}+\underline{2}$$
$$\underline{37}=18\times\underline{2}+\underline{1}$$
$$\underline{2}=2\times\underline{1}$$

得$(3824,\ 1837)=1$，故$(-3824,\ 1837)=1$.

定理 1 设 a，b 是两个不全为零的整数，则存在两个整数 u，v，使

$(a,\ b)=ua+vb$.

证明：设 Z 是全体整数集合. 做一个如下集合：

$$S=\{|xa+yb|\ |x,\ y\in Z\}.$$

S 中的元素显然大于等于 0.

设 d 是 S 中的最小正整数，则 d 可表示为 a，b 的组合，设

$$d=ua+vb.$$

现在我们证明 $d|a$ 且 $d|b$.

做带余除法：

$$a=qd+r,\ 0\leqslant r<d.$$

于是

$$r=a-qd=a-q(ua+vb)=(1-qu)a-qvb.$$

这说明 r 也可表示为 a，b 的组合，则 $r\in S$. 由于 d 是 S 中的最小正整数，所以只有 $r=0$. 故 $d|a$. 同理 $d|b$.

设 c 是 a，b 的任意公因子，由 $c|a$ 和 $c|b$ 得 $c|d=ua+vb$. 故 d 是 a，b 的最大公因子，证毕.

定理 1 表明 a，b 的最大公因子可以表示为 a，b 的组合. 实际上，从欧几里得除法求最大公因子的过程也可以看出$(a,\ b)$可表示为 a，b 的组合：

r_2 可表示为 $r_0=a$，$r_1=b$ 的组合，

r_3 可表示为 r_1，r_2 的组合，

…

r_n 可表示为 r_{n-1}，r_{n-2} 的组合，

所以 $r_n=(a,\ b)$ 可表示为 a，b 的组合.

例 6 将 $a=888$，$b=312$ 的最大公因子表示为$(a,\ b)=ua+vb$.

解 利用欧几里得除法求最大公因子的过程可以解出.

由

$$\underline{888}=2\times\underline{312}+\underline{264}$$
$$\underline{312}=1\times\underline{264}+\underline{48}$$
$$\underline{264}=5\times\underline{48}+\underline{24}$$

我们有

$$264=888-2\times312$$
$$48=312-264=312-(888-2\times312)=-888+3\times312$$
$$24=264-5\times48=(888-2\times312)-5\times(-888+3\times312)=6\times888-17\times312$$

故$(888,\ 312)=24=6\times888-17\times312$.

定义 3 设 a，b 是两个不全为 0 的整数，如果$(a,\ b)=1$，则称 a，b **互素**.

推论 a，b 互素的充分必要条件是：存在 u，v，使

$$ua+vb=1.$$

证明：必要条件是定理 1 的特例，只需证充分条件.

如果存在 u，v，使

$$ua+vb=1.$$

则由$(a,\ b)|(ua+vb)$，得$(a,\ b)|1$，所以$(a,\ b)=1$.

例 7 由例 5 知 $a=-3824$，$b=1837$ 互素，求 u，v，使 $ua+vb=1$.

解：方法同例 6.

由

$$3824 = 2\times 1837+150$$
$$1837 = 12\times 150+37$$
$$150 = 4\times 37+2$$
$$37 = 18\times 2+1$$

我们有

$$150 = 3824-2\times 1837$$
$$37 = 1837-12\times 150 = -12\times 3824+25\times 1837$$
$$2 = 150-4\times 37 = 49\times 3824-102\times 1837$$
$$1 = 37-18\times 2 = -894\times 3824+1861\times 1837$$

故 $894\times(-3824)+1861\times 1837 = 1$，$u = 894$，$v = 1861$.

互素有如下性质：

（1）如果 $c\mid ab$ 且$(c, a) = 1$，则 $c\mid b$.

（2）如果 $a\mid c$，$b\mid c$，且$(a, b) = 1$，则 $ab\mid c$.

（3）如果$(a, c) = 1$，$(b, c) = 1$，则$(ab, c) = 1$.

证明：（1）因为$(c, a) = 1$，存在 u，v，使

$$ua+vc = 1,$$

两端乘 b 得

$$uab+vcb = b.$$

由于 $c\mid uab+vcb$，故 $c\mid b$.

（2）因为$(a, b) = 1$，存在 u，v，使

$$ua+vb = 1,$$

两端乘 c 得

$$uac+vbc = c.$$

由 $a\mid c$，$b\mid c$，得 $ab\mid uac$，$ab\mid vbc$，故 $ab\mid c$.

（3）因为$(a, c) = 1$，存在 u，v，使

$$ua+vc = 1,$$

因为$(b, c) = 1$，存在 r，s，使

$$rb+sc = 1,$$

于是

$$(ua+vc)(rb+sc) = (ur)ab+(usa+vrb+vsc)c = 1.$$

故$(ab, c) = 1$.

定义 4　设 a，b 是两个不等于零的整数. 如果 $a\mid d$，$b\mid d$，则称 d 是 a 和 b 的**公倍数**. a 和 b 的正公倍数中最小的称为 a 和 b 的**最小公倍数**，记为$[a, b]$.

由定义显然有

$$[a, b] = [-a, b] = [a, -b] = [-a, -b].$$

例 8　$a = 2$，$b = 3$. 它们的公倍数集合为

$$\{0, \pm 6, \pm 12, \pm 18, \cdots\}.$$

而[2，3]=6.

定理2 （1）设 d 是 a，b 的任意公倍数，则

$$[a，b]\mid d.$$

（2）$[a，b]=\dfrac{|ab|}{(a，b)}$．特别地，如果$(a，b)=1$，$[a，b]=|ab|$.

证明：（1）做带余除法：

$d=q[a，b]+r$，$0\leqslant r<[a，b]$，

由于 $a\mid d$，$b\mid d$，以及 $a\mid[a，b]$，$b\mid[a，b]$，则 $a\mid r$，$b\mid r$，r 也是 a，b 的公倍数，这与$[a，b]$是 a，b 的最小公倍数相矛盾，所以 $r=0$，故$[a，b]\mid d$.

（2）不失一般性，假设 a，b 均是正整数．我们现在证明$\dfrac{ab}{(a，b)}$是 a，b 的公倍数而且对于 a，b 的任意公倍数 d 都有

$$\frac{ab}{(a，b)}\Bigg| d\ .$$

设 $a=k_a(a，b)$，$b=k_b(a，b)$，其中$(k_a，k_b)=1$．则

$$\frac{ab}{(a，b)}=k_ab=k_ba.$$

所以$\dfrac{ab}{(a，b)}$是 a，b 的公倍数.

设 a，b 的任意公倍数 $d=q_aa=q_bb$，于是

$$d=q_ak_a(a，b)=q_bk_b(a，b).$$

$$q_ak_a=q_bk_b.$$

因为$(k_a，k_b)=1$，则

$$k_a\mid q_b.$$

$$k_ab\mid q_bb=d.$$

$$\frac{(a，b)k_ab}{(a，b)}\Bigg| d\ ,$$

$$\frac{ab}{(a，b)}\Bigg| d\ .$$

这表明$\dfrac{ab}{(a，b)}$是公倍数中最小的，定理得证.

由定理2可以得到求最小公倍数的方法：先利用欧几里得除法求出最大公因子，然后由定理2就可以求出最小公倍数了.

例9 $a=888$，$b=312$，求$[a，b]$.

解：$(888，312)=24$，则$[888，312]=\dfrac{888\times312}{24}=11\,544$.

1.2 素数

定义 1 如果一个大于 1 的整数 p 除±1 和±p 外无其他因子，则 p 称为一个**素数**，否则称为**合数**.

例 1 2，3，5，7，11，13，17，19 都是素数，而 4，6，8，10，12，14，15，16，18，100 都是合数.

定理 1 设 p 是一个素数，则

（1）对任意整数 a，如果 p 不整除 a，则$(p, a) = 1$.

（2）如果 $p \mid ab$，则 $p \mid a$，或 $p \mid b$.

证明：（1）因为$(p, a) \mid p$，由素数的定义，$(p, a) = 1$，或者$(p, a) = p$. 因为 p 不整除 a，所以 $(p, a) \neq r$.故$(p, a) = 1$.

（2）如果 $p \mid a$，则成立. 否则$(p, a) = 1$，则由互素的性质，有 $p \mid b$.

下面给出非常重要的**算术基本定理**，该定理由两千多年前的古希腊数学家所发现.

定理 2 （算术基本定理）每个大于 1 的整数 a 都可以分解为有限个素数的乘积：

$$a = p_1 p_2 \cdots p_r.$$

该分解除素数因子的排列外是唯一的.

证明：分解是显然的，我们只需证明分解除素数因子的排列外是唯一的.

假设 a 有两个分解：

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

由于 $p_1 \mid q_1 q_2 \cdots q_s$，则 p_1 整除 q_1，q_2，…，q_s 之一，不失一般性，假设 $p_1 \mid q_1$，由 p_1，q_1 都是素数得 $p_1 = q_1$. 在等式两边消去 p_1，q_1，得

$$p_2 \cdots p_r = q_2 \ldots q_s.$$

重复上述过程可得 $p_1 p_2 \cdots p_r$ 和 $q_1 q_2 \cdots q_s$ 除排列外是相同的，证毕.

由于 p_1，p_2，…，p_r 中可能存在重复，所以 a 的分解式可表示为有限个素数的幂的乘积：

$$a = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}.$$

这称为 a 的**标准因子分解式**.

例 2 900 的标准因子分解式：

$$900 = 2 \times 2 \times 3 \times 3 \times 5 \times 5 = 2^2 \times 3^2 \times 5^2.$$

整数的素因子分解没有一个一般的方法，当整数很大时，其分解会变得非常困难，这就是大数分解难解问题，是构造公钥密码的重要基础之一.

定理 3 设 a 是任意大于 1 的整数，则 a 的除 1 外最小正因子 q 是一素数，并且当 a 是一合数时，

$$q \leqslant \sqrt{a}.$$

证明：由算术基本定理，该定理的前一点是显然的.

当 a 是一合数时，可设

$$a = a_1 q，\text{其中 } a_1 \geqslant q.$$

则

$$a = a_1 q \geqslant q^2,$$
$$\sqrt{a} \geqslant q .$$

定理证毕.

我们下面介绍求不超过一个正整数 N 的全部素数的有效方法——古老的 **Eratosthenes 筛法**. 该方法是古希腊数学家 Eratosthenes 发明的，其原理建立在定理 3 之上. 我们用 $N = 100$ 这个具体例子来介绍 Eratosthenes 筛法.

求不超过 100 的全部素数.

第 1 步　找出 $\leqslant \sqrt{100} = 10$ 的全部素数：2，3，5，7.

第 2 步　在 1～100 中分别划去第 1 步找出的每个素数的全部倍数：分别划去 2 的全部倍数、3 的全部倍数、5 的全部倍数和 7 的全部倍数（本身除外）.

（1）划去 2 的全部倍数：

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~~

得到剩下的数：

1	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

（2）划去 3 的全部倍数：

1	2	3	5	7	~~9~~
11		13	~~15~~	17	19
~~21~~		23	25	~~27~~	29
31		~~33~~	35	37	~~39~~
41		43	~~45~~	47	49