1 起源：从 Euclid 到 Chebyshev

0. 引论

数数, 首先是在自己身上数. 这当然是比喻的说法, 但其本意也是如此：人们用手指、脚趾、肩、膝盖等数数. 从词源学的角度来看, 各种数字的叫法实际上是一些非常古老的语言的遗迹. 在这些语言里, 不同数字的称谓对应着人体的不同部位. 数作为我们描绘这个世界的原始模型, 在最强烈的意义下构成了我们的一部分, 以致我们可以合乎情理地问自己数论的研究对象是否就是人类思想本身. 由此产生一个奇怪的困惑：这些同我们息息相关的数字, 怎么会产生如此令人生畏的谜团？在所有这些谜团中, 有关素数的问题可能是其中最古老同时也是最困难的一个. 我们这本小书的目的就在于向读者介绍人类为理解这个难题所发明的一些方法. 但愿这些相互关联的奥秘能用来度量我们无知的程度, 并由此产生对知识难以满足的渴望!

从本质上讲, 有两种方法将整数结合起来. 事实上我们可以对整数进行相加和相乘. 利用加法, 我们能借助较小的整数来获得事先固定的任何整数. 然而对于乘法, 人们会很快发现, 为从较小的整数来获得事先固定的整数, 此时必须时不时地引入一些无法约化为前面元素的新元素. 这些新元素被称为素数. 从蒙昧时代开始, 人类就一直在试图穷其究竟 ·····

素数集就这样开始：

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,$$

$$59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97,\ 101,\ \cdots,\ 571,\ \cdots$$

大约 23 世纪以前, Euclid 证明了素数集是无限的. 若采用现代记号, 他的简单优美的证明可表示成四个符号：

$$n!+1.$$

事实上, 该数不能被任何满足 $2 \leqslant d \leqslant n$ 的整数 d 所整除; 因此它只有大于 n 的素因子. 这就证明了对于预先给定的任何界限, 都至少存在一个素数比它大.

对任意实数 $x>0$, 记 $\pi(x)$ 为不大于 x 的素数 p 的个数, 即

$$\pi(x)=\sum_{p\leqslant x} 1.$$

Euclid 的结果表明 $\pi(x)$ 随着 x 一起趋向于无穷. 由此向人们提出一个对该函数的增长速度进行研究的问题.

直到 18 世纪, 才由 Euler 在该领域获得了一个真正的突破. 事实上, 他发现了下面将一个对所有整数进行的求和式与一个对所有素数进行的无穷乘积联系在一起的基本公式

$$\sum_{n=1}^{\infty}\frac{1}{n^{\sigma}}=\prod_{p}\frac{1}{1-p^{-\sigma}}\quad(\sigma>1).$$

尽管该公式在 $\sigma=1$ 时不成立, 但 Euler 仍毫不犹豫地给它赋予了下面的意义[1)]

$$\prod_{p}(1-1/p)=0.$$

由 $\log(1-1/p)$ 与 $-1/p$ 同阶, Euler 得出素数的倒数和发散：

$$\sum_{p}1/p=\infty.$$

该计算将会在第 5 节中得到证明和精确化.

[1)] 按照当今的术语, 我们可称之为连续延拓.

首先是 Gauss (1792), 随后是 Legendre (1798, 1808), 他们均猜想当 x 趋近于无穷时,

$$\pi(x) \sim x/\log x.^{1)}$$

在几十年后的 1852 年, Chebyshev 证明了该猜想的一个弱形式：存在常数 a 和 b 使得

$$ax/\log x < \pi(x) < bx/\log x \quad (x \geqslant 2).$$

从数值的角度来看, 上述结论为 Gauss-Legendre 猜想提供了一个非常有说服力的证据：事实上, 对于充分大的 x, 我们可以选取 $a = 0.921$ 和 $b = 1.106$.

Riemann (1859) 创造性地将 zeta 函数

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

延拓成复变量函数. 这使得 $\zeta(s)$ 在其级数的收敛区域之外也可以有意义. 正如 Riemann 所证明的那样, 对该延拓的研究能很快地给出与 $\pi(x)$ 有关的信息.

最后, Hadamard 和 La Vallée-Poussin 各自借助 Riemann 的研究成果, 于 1896 年独立地证明了素数定理

$$\pi(x) \sim x/\log x \quad (x \to \infty).$$

本书在某种程度上记录了这段历史. 大家将会看到, 对该问题的研究还远远没有结束.

1. 素数分解

一个素数是一个严格大于 1 的整数 p 并且该整数没有任何因子 d 满足 $1 < d < p$. 可见 1 不是素数, 而 2 是唯一的偶素数.

正如我们在上一节中所指出的那样, 素数之所以处于数论研究的中心位置是基于如下事实：如果不考虑因子的顺序, 任何严格大于 1 的整数 n 均可

1) 值得注意的是, 该式等价于第 n 个素数的渐进公式 $p_n \sim n \log n$.

以唯一地分解成素数的乘积

$$n=\prod_{j=1}^{k}p_j^{\nu_j}.$$

该分解的存在性几乎是显然的：为此只需利用归纳法进行讨论. 若该性质对所有 $<n$ 的整数均成立并且若 n 不是素数, 那么 n 有一些因子 $d\in(1,\,n)$. 对于任何一个这样的因子, 我们可以将 n 分解成 $n=dm$, 其中 $m=n/d\in(1,\,n)$. 此时对 d 和 m 分别运用归纳假设条件便可得到所要的结果.

唯一性的问题很不容易处理. 它需要应用*Euclid* 第一定理：若素数 p 整除乘积 ab, 则 p 整除 a 或 b. 暂时承认该定理. 那么, 如果 n 有两个不同的素因子分解 $n=\prod_{j=1}^{k}p_j^{\nu_j}$ 和 $n=\prod_{i=1}^{\ell}q_i^{\sigma_i}$, 则每个 p_j 必等于某个 q_i, 反过来也是如此. 特别地, 我们有 $k=\ell$, 并且在将因子进行适当地重新编号后, 可得 $p_j=q_j$ $(1\leqslant j\leqslant k)$. 再假设, 比如说 $\nu_1>\sigma_1$. 则 $m=n/p_1^{\sigma_1}$ 有两个与不同的素数集相对应的分解. 这与证明的第一部分相矛盾.

Euclid 第一定理的现代证明需借助于人们对整数集 $\mathbb{Z}$ 的理想的结构的了解. 我们称非空子集 I 是 $\mathbb{Z}$ 的一个理想, 若它在减法运算以及与任何一个整数相乘的运算下均保持不变, 换句话说：

$$(x\in I,\ y\in I)\Rightarrow x-y\in I,\quad (x\in\mathbb{Z},\ y\in I)\Rightarrow xy\in I.$$

容易看到所有的倍数集

$$\alpha\mathbb{Z}=\{\alpha m:\ m\in\mathbb{Z}\}$$

均为 $\mathbb{Z}$ 的理想. 其逆命题更加令人震惊：集合 $\mathbb{Z}$ 的任意一个理想 I 都是一个倍数集 $I=\alpha\mathbb{Z}$. 事实上, 不退化为 $\{0\}$ 的理想 I 包含正元：由定义理想的那两条性质中的任何一个均可导出 I 在映射 $x\mapsto -x$ 下保持不变. 设 α 为 I 中的最小正元, 那么 $\alpha\mathbb{Z}\subset I$. 反过来, 对任意的 $\beta\in I$, 由 Euclid 除法可得 $\beta=\alpha q+r$, 其中 $0\leqslant r<\alpha$. 但 $\alpha q\in I$, 于是有 $r=\beta-\alpha q\in I$. 再由 α 的最小性, 可知必有 $r=0$ 及 $\beta=\alpha q\in\alpha\mathbb{Z}$.

我们现在证明 Euclid 第一定理. 设 a, b, p 满足 $p\mid ab$ 和 $p\nmid a$. 由所有线性组合 $ax+py$ $(x,\ y\in\mathbb{Z})$ 所组成的集合 $a\mathbb{Z}+p\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个理想 $\alpha\mathbb{Z}$. 该理想包含 a 和 p, 因此有 $\alpha\mid a$ 和 $\alpha\mid p$. 由后一条件可得 $\alpha=1$ 或 $\alpha=p$. 但 $p\nmid a$, 所以第二种可能性可被排除. 由此得 $\alpha=1$, 从而 $a\mathbb{Z}+p\mathbb{Z}=\mathbb{Z}$. 特别地, 存在

$x,\ y\in\mathbb{Z}$ 使得

$$ax+py=1.\ ^{1)}$$

在等式的两边同乘以 b, 得 $b=abx+pby=p\{(ab/p)x+by\}$, 从而有 $p\mid b$, 这就是所要证明的.

2. 同余

同余的概念要归功于 Gauss. 设 m 为 $\geqslant 1$ 的整数. 两整数 $x,\ y$ 被称为模 m 同余, 若它们的差 $x-y$ 能被 m 整除. 此时记作

$$x\equiv y\,(\mathrm{mod}\,m).$$

与给定的整数 a 同余的所有整数的集合叫作 a 的同余类, 记作 $\overline{a}$. 同余类 $\overline{a}$ 中的任意一个元素被称为 $\overline{a}$ 的*代表元*. 每一个同余类在集合 $\{0,\,1,\,\cdots,\,m-1\}$ 中有唯一的代表元, 而任意一个整数 n 在该集合中的代表元等于该整数被 m 除后的余数. 由所有同余类组成的集合记作 $\mathbb{Z}/m\mathbb{Z}$ [2)], 并且我们还可以验证, 对任意的整数 $a,\ b$, 同余类 $\overline{a+b}$ 和 $\overline{ab}$ 仅依赖于 a 和 b 各自所在的同余类. 因此我们可以给 $\mathbb{Z}/m\mathbb{Z}$ 赋予如下定义的加法和乘法：

$$\overline{a}+\overline{b}=\overline{a+b},\quad \overline{a}\overline{b}=\overline{ab}.$$

这些运算[3)] 使得 $\mathbb{Z}/m\mathbb{Z}$ 带上了一个交换幺环的结构：换句话说, 这些计算规则同 $\mathbb{Z}$ 中的是一样的. 然而, 这些规则不能被推广到除法：$\mathbb{Z}/m\mathbb{Z}$ 通常不是整的, 也就是说两个非零元素的乘积可以为零. 例如在 $\mathbb{Z}/6\mathbb{Z}$ 中就有 $\overline{2}\times\overline{3}=\overline{0}$. 我们用 $(\mathbb{Z}/m\mathbb{Z})^*$ 表示 $\mathbb{Z}/m\mathbb{Z}$ 中所有可逆元组成的集合, 即：使方程 $\overline{ax}=\overline{1}$ 有解的同余类 $\overline{a}$ 所组成的集合. 传统上将 Euler *示性函数* 记作 $\varphi(m)$, 其定义为

$$\varphi(m)=|(\mathbb{Z}/m\mathbb{Z})^*|.\ ^{4)}$$

---

1) 该结论叫作*Bachet 定理* (1624). 但它通常被错误地归在 Bézout 的名下.

2) 因此在 $\mathbb{Z}/m\mathbb{Z}$ 与任何一个长度为 m 的整数区间 (例如 $\{0,\ 1,\ \cdots,\ m-1\}$) 之间存在着自然双射.

3) 习惯上去掉 $\mathbb{Z}/m\mathbb{Z}$ 中的等价类上的横杠. 同样地, 即使实际上是在对等价类进行计算, 我们也通常用它们在 $\mathbb{Z}$ 中的代表元来表示. 此时用同余号代替等号, 并且还要在所表达的关系式中添加 $(\mathrm{mod}\,m)$.

4) 提醒一下, 我们用 $|A|$ 来表示有限集 A 的元素的个数.

大家可马上注意到, 对每个整数 $m \geqslant 1$, $\varphi(m)$ 等于与m 互素的整数 a $(1 \leqslant a \leqslant m)$ 的个数. 以后我们还会回到 $\varphi(m)$ 的性质上来.

为此, 可设 $N(m)$ 为与 m 互素的所有整数 a $(1 \leqslant a \leqslant m)$ 的个数. 由 $ax \equiv 1 \pmod m$ 可知 $(a, m) = 1$, 进而可得 $\varphi(m) \leqslant N(m)$. 反过来, 若 $(a, m) = 1$, 对 m 的所有素因子 (重数也考虑在内) 运用 Bachet 定理, 并将由此得到的所有相应的关系式 $ax + py = 1$ 相乘, 可得 $aX + mY = 1$, 其中 X, Y 为适当的整数. 这就正好导出了 $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$.

由上面这个 Bachet 定理的应用而得到的一个重要推论是：对任意素数 p, 集合 $\mathbb{Z}/p\mathbb{Z}$ 是一个域. 换句话说：任意一个不是 p 的倍数的整数 a 的同余类在 $\mathbb{Z}/p\mathbb{Z}$ 中可逆. 由于 $a \not\equiv 0 \pmod p$ 等价于 $(a, p) = 1$, 因此该结论可立刻由前面的证明推出. 特别地, 对任意素数 p, $\mathbb{Z}/p\mathbb{Z}$ 是整的并且 $\varphi(p) = p - 1$. 大家将会在第 1 章第 6 节中看到, 更一般地, 对任意的 $n \geqslant 1$, 我们有

$$\varphi(n) = n \prod_{p|n} (1 - 1/p).$$

由前面的讨论, 我们还可得出次数为 d 的整系数多项式方程

$$P(x) \equiv 0 \pmod p$$

在 $\mathbb{Z}/p\mathbb{Z}$ 中至多有 d 个不同根这一基本结论.

为此, 假设方程有 k 个不同的根 $x_1, \cdots, x_k$. 由 $P(x) = P(x) - P(x_1)$ 并有步骤地运用恒等式

$$x^j - x_1^j = (x - x_1) \sum_{i=0}^{j-1} x_1^i x^{j-1-i} \quad (1 \leqslant j \leqslant d),$$

可得 $P(x) \equiv (x - x_1)^{a_1} Q_1(x) \pmod p$, 这里 $a_1 \geqslant 1$, 而 $Q_1(x)$ 是一个次数为 $d - a_1$ 的多项式并且 x_1 不是它的根. 因此 x_2 必为多项式 $Q_1(x)$ 的根. 重复上述过程可得

$$P(x) \equiv \prod_{j=1}^{k} (x - x_j)^{a_j} Q_k(x) \pmod p,$$

其中 Q_k 是一个在 $\mathbb{Z}/p\mathbb{Z}$ 中无根的多项式, 并且其最高次项的系数与 $P(x)$ 的最高次项的系数相同. 由此可得

$$k \leqslant \sum_{1 \leqslant j \leqslant k} a_j \leqslant d.$$

设 p 为一素数, a 为一整数但不是 p 的倍数. 考虑 $(\mathbb{Z}/p\mathbb{Z})^*$ 上的映射 $x \mapsto ax$. 这是一个单射, 但由于所讨论的集合是有限的, 所以它也是双射. 从而

$$\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x = \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} ax = a^{p-1} \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x,$$

由此导出

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p) \quad (a \in (\mathbb{Z}/p\mathbb{Z})^*).$$

这个重要的恒等式称作*Fermat 小定理* [1]. 另外, 可以很容易地将它推广到环 $(\mathbb{Z}/m\mathbb{Z})^*$ 的情形 (其中 m 为任意整数)：若 $a \in (\mathbb{Z}/m\mathbb{Z})^*$, 则映射 $x \mapsto ax$ 将 $(\mathbb{Z}/m\mathbb{Z})^*$ 中的元素进行置换. 经过同样的计算可得 (这一次利用 $(\mathbb{Z}/m\mathbb{Z})^*$ 中的可逆元的乘积还是可逆的)

$$a^{\varphi(m)} \equiv 1 \,(\mathrm{mod}\, m) \quad (a \in (\mathbb{Z}/m\mathbb{Z})^*).$$

这就是著名的*Euler 公式*.

设 n 为奇数. 大家在下节中会看到, 即使对于取值很大的 n, 对 $2^{n-1} \,(\mathrm{mod}\, n)$ 的数值计算仍是非常快的. 若该量不等于 1, 则 n 不是素数. 若它等于 1, 虽然这并不意味着 n 为素数, 但例外的情形 (此时称 n 是*以 2 为底的伪素数*) 却是很少的. 这个注记是一些用来判断整数是否为素数的现代检测方法的基石.

Fermat 小定理没有真正意义上的逆命题[2]. 我们称整数 $n > 1$ 是一个*Carmichael 数*, 如果 n 是一个合数 (即不是素数) 并且对任意与 n 互素的整数 a, 都有 $a^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$. 最小的 Carmichael 数为 561. Alford, Granville 和 Pomerance 在 1992 年证明了存在着无穷多个 Carmichael 数.

$\mathbb{Z}/p\mathbb{Z}$ 为域这一事实的另一推论是*Wilson 定理* (于 1770 年发表在 Waring 的一篇文章中)：

---

[1] 以区别于著名的*Fermat 大定理*. 后者是说当 $n \geqslant 3$ 时, 方程 $x^n + y^n = z^n$ 没有非零的整数解 x, y, z. 这个始于 1638 年左右的晦涩命题, 最近刚由 Wiles 和 Taylor 所证明 (1994) $\cdots$, 但这完全是另外一个故事了.

[2] 其间 Lucas (1891) 证明了, 若 $(a, n) = 1$, $a^{n-1} \equiv 1 \,(\mathrm{mod}\, n)$ 并且对于 $n-1$ 的任意素因子 q 均有 $a^{(n-1)/q} \not\equiv 1 \,(\mathrm{mod}\, n)$, 则 n 也是一个素数. 该结果常被用来生成大素数.

$$p \text{ 为素数} \Leftrightarrow (p-1)!+1 \equiv 0 \,(\mathrm{mod}\, p).$$

条件是充分的：若 $q \mid p$ 且 $1 \leqslant q < p$, 则 $q \mid (p-1)!$, 这意味着 $q \mid 1$, 从而 $q = 1$. 它也是必要的：乘积 $(p-1)! \equiv \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x \,(\mathrm{mod}\, p)$ 中的每一项 x 都有一个模 p 的逆元 x', 并且 $x = x'$ 当且仅当 $x \equiv 1 \,(\mathrm{mod}\, p)$ 或 $x \equiv p-1 \,(\mathrm{mod}\, p)$. 将乘积中的各项进行分组, 使得当 $x \neq x'$ 时, x 与它的逆元 x' 放在一起, 由此可得原乘积同余于 $1 \times (p-1) \equiv -1 \,(\mathrm{mod}\, p)$.

3. 密码间奏曲：公钥密码系统

二十多年来, 各种新的密码方法不断涌现, 其间数学 (特别是素数理论) 起了决定性作用, 这使得民政部门与军事机构对素数的兴趣大幅度地增长.

随着计算机科学的迅猛发展以及对各种信息传输进行保密的需要, 大量的资金被投入到这些应用上来. 永恒不变的赢利法则推动了该领域内的研究, 各种成果, 包括理论上的, 凭借着各种有利条件而大量涌现. 判断整数素性的准则, 素因子分解的算法, 素数的生成方法以及其他概念性的专门化设计, 也随之在校园里蓬勃发展起来.

当然, 在所有这些里面, 并没有什么精神上的东西, 但我们也许仍可以从中感悟一种 (双重的) 寓意：金钱确实可以促进科学的进步; 与此同时, 如果在可望立刻获得经济效益的前题下所取得的进步是十分巨大的, 那么我们是否能够期望得到一些即便是非常微弱的赞助, 来用于一个中期或长期的基础性研究呢?

我们在这里仅简单扼要地描述一下 “RSA 系统”[1]. 该系统提供了一个几乎无法破译却又十分简单的编码技术.

考虑由 n 个人 $\{I_1, I_2, \cdots, I_n\}$ 组成的网络系统. 系统中的成员彼此之间以*加密* (加密后的邮件不能被收件者以外的人看到) 或*赋予数字签名* (赋予了数字签名的邮件也许能被所有的人看到, 但却无法被伪造) 的方式进行交流. 为此, 系统 RSA 给网络中的每个成员 I_j 分配一对素数 (p_j, q_j) —— 也就是说可分解成两素数乘积的整数 $n_j = p_j q_j$ —— 以及一个与 $\varphi(n_j) = (p_j - 1)(q_j - 1)$

[1] 指 Rivest, Shamir 和 Adleman. 他们在 1978 年发表的那篇文章标志着该研究领域的一个重大转折.

互素的整数 c_j. RSA 系统之所以能够成功地实现其保密目的是基于如下事实：就目前的计算手段而言, 很容易生成“大”素数 (因此能给网络成员提供足够的 p_j 和 q_j), 但几乎不大可能分解一个大小为这些素数平方的整数 (即从 n_j 重新得到 p_j 和 q_j). 在本书的撰写阶段, 阶为 10^{100} 的素数在这个特殊意义下可被看作是“大的”.

RSA 网络系统附带一个 (公开的) 用户目录, 其上给出了与每个 I_j 相对应的 n_j 和 c_j. 然而只有 I_j 知道 n_j 的素数分解, 从而也只有他才能直接找到 c_j 模 $\varphi(n_j)$ 后的逆元 d_j [1)].

一条消息就是一个不大于那些 n_j (它们基本上是同阶的) 的整数 M, 或等价地说是一串这样的整数：例如只需将每个字母用它在字母表中的次序来代替, 并将所得到的两位数整数串在一起.

比如说当 I_1 想给 I_2 发一条加了密的消息 M 时, 他就给 I_2 寄去整数 $M_2 = M^{c_2} \pmod{n_2}$, 也就是说 M_2 为 $\equiv M^{c_2} \pmod{n_2}$ 的最小正整数. 当 I_2 收到 M_2 时, 他只需利用 Euler 公式[2)] 来计算 $M_2^{d_2} \equiv M \pmod{n_2}$. I_2 就这样破解了 I_1 所发来的消息. 由于仅借助用户目录所提供的数据 (事实上) 是不可能计算出 d_2 的, 因而其他人均无法破译该消息.

当 I_1 打算给 I_2 发一条赋予了数字签名的消息 M 时, 他就给 I_2 寄去整数 $M_1 = M^{d_1} \pmod{n_1}$. 而 I_2 (实际上该网络中的任何成员) 可以 (同样借助于 Euler 公式) 算出 $M_1^{c_1} \equiv M \pmod{n_1}$. 由于该解码过程提供了一条前后语义连贯的消息, 这就说明只能是 I_1 进行了上述加密. 由此可知 M 确实已被赋予了数字签名.

当 I_1 想给 I_2 发一条既加了密同时又被赋予了数字签名的消息 M 时,

[1)] 对逆元的数值计算是非常快的, 所需运算的次数仅与涉及的整数的位数同阶. 不失一般性, 考虑两整数 a 和 b 使得 $1 \leqslant a < b$ 且 $(a, b) = 1$. 若 q_1 是与 b/a 最接近的整数, 则 $r_1 := b - aq_1$ 满足 $|r_1| \leqslant a/2$. 同样地, 存在整数 q_2 使得 $r_2 := a - r_1 q_2 = a(1 + q_1 q_2) - bq_2$ 满足 $|r_2| \leqslant a/4$. 重复以上过程并记 $r_{j+1} = r_{j-1} - r_j q_{j+1}$, 则 $|r_{j+1}| \leqslant a/2^{j+1}$. 经过至多 $(\log 2a)/\log 2$ 步后, 可得 $r_{k+1} = 0$, 从而 $r_k \mid r_{k-1}$. 容易验证由此可导出 $r_k \mid (a, b)$, 进而 $r_k = \pm 1$. 但由以上构造可知 r_k 是 a 和 b 的一个线性组合. 这样就找到了整数 u 和 v 使得 $au + bv = \pm 1$. 因而 a 模 b 后的逆元为 u 或 $b - u$.

[2)] 我们有 $c_2 d_2 \equiv 1 \pmod{\varphi(n_2)}$, 因此 $(M, n_2) = 1$ 时 $M_2^{d_2} \equiv M \pmod{n_2}$. 可以证明这个关系式即使在 $(M, n_2) > 1$ 时也同样成立.

若此时比如说有 $n_1 < n_2$, 他就将 $M_{12} = M_1^{c_2} \pmod{n_2}$ 寄给 I_2. 而 I_2 则可以通过依次计算整数 $M_{12}^{d_2} \equiv M_1 \pmod{n_2}$ 和 $M_1^{c_1} \equiv M \pmod{n_1}$ 来破译该消息 —— 至于数字签名就由上述过程的第二步所提供的消息是可读的这一简单事实来得到保证.

需要提醒的是, 高阶幂 M^c 对一个 N 位 (目前 $N \approx 200$) 整数 n 求同余的计算并不需要很复杂的计算工具. 事实上, M^2 关于模 n 求同余的计算对应于两个 N 位数间的乘法, 并显然给出一个 N 位数的结果. 这意味着当 $c = 2^k$ 时, M^c 关于模 n 求同余的计算对应于做 k 次两个 N 位数之间的乘法, 而在一般情形, 由二进制展式 $c = \sum_{0 \leqslant j \leqslant k} \varepsilon_j 2^j$ (其中 $\varepsilon_j = 0$ 或 1) 可知至多需 $k \ll N$ 次乘法. 对于那些不超过几百的整数 N, 就当今计算机的运行速度而言, 加密过程几乎可以在瞬间完成.

4. 二次剩余

设 p 为一奇素数. 考虑由 $q(x) = x^2$ 所定义的映射

$$q : \ (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*.$$

则 q 为积性同态, 也就是说, 恒有

$$q(xy) = q(x)q(y).$$

由于方程 $q(x) = 1$ 恰有两个解, 即 1 和 $p-1$ (也可以说成是 ± 1, 这是因为在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中有 $p - 1 = -1$), 可见如果方程 $q(x) = a$ 有一个解, 比如说是 x_1, 那么该方程正好有两个解 x_1 和 $p - x_1$. 这样的数 a 称为模 p 的二次剩余. 由上可知恰有 $\frac{1}{2}(p-1)$ 个模 p 的二次剩余. 事实上, 若用 Q_p 表示模 p 的所有二次剩余的集合, 那么这 $|Q_p|$ 个二元子集 $q^{-1}\{a\} = \{x \in (\mathbb{Z}/p\mathbb{Z})^* : \ q(x) = a\}$ $(a \in Q_p)$ 构成了 $(\mathbb{Z}/p\mathbb{Z})^*$ 的一个分割, 由此得 $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*| = 2|Q_p|$.

考虑满足 $f(x) = x^{(p-1)/2}$ 的积性同态 $f : \ (\mathbb{Z}/p\mathbb{Z})^* \to \{-1, 1\}$. 由 Fermat 小定理可知, 对 Q_p 中的任意 a, 有 $f(a) = 1$, 又因为多项式方程 $f(x) = 1$ 在 $(\mathbb{Z}/p\mathbb{Z})^*$ 中至多有 $\frac{1}{2}(p-1)$ 个根, 因而 Q_p 正好就是这些根的集合. 也就是说