arXiv:2603.13939v1 [math.NT] 14 Mar 2026

与群变体相关的欧拉函数

James Renshaw 数学科学学院，南安普顿大学，南安普顿，SO17 1BJ，英格兰。ORCID：0000-0002-5571-8007 电子邮箱：j.h.renshaw@soton.ac.uk

2026年3月

摘要

受半群变体在群上的离散对数问题及相关密码学应用中的应用所启发，我们引入了一种新型欧拉函数，它既与欧拉函数有关，也与 Schemmel 于 1869 年引入的欧拉函数推广形式有关。我们重点探讨如何计算这一函数；相关数论虽然并非平凡，有时也略显技术性，但对广大读者而言仍相当易于理解。此外，读者也会发现，这一新函数显然存在一些推广形式，感兴趣的读者或许愿意进一步研究。

数学主题分类：11A05，11A25，20A05，20M10 关键词：欧拉函数、群变体、离散对数问题。

1 引言

假设我们以 PDF 文件的形式下载本文内容，并希望对其进行加密。当然，现有许多广为人知且有效的加密方案，但我们希望探讨一种基于群变体以及一种与欧拉函数相关的新型欧拉函数的方案。我们将此函数定义为 T：$\mathbb{N} \to \mathbb{N}$，其中令 $T(n)$ 表示满足以下条件的奇单位的个数：$m \in \mathbb{Z}_n$ 使得 $(m-1)/2$ 也是一个单位，其中 $\mathbb{Z}_n$ 是模 n 的整数环。回顾一下，单位是一个正整数 $m \in \mathbb{Z}_n$，满足存在 $m' \in \mathbb{Z}_n$ 使得 $mm' \equiv 1$ 模 (n)，或者等价地，$\gcd(m, n) = 1$。我们将看到 $T(n)$ 的值与我们系统的安全性有何关系。

作为一个具体例子，令 p 为一个安全素数，也就是说，它是形如 $p = 2q+1$ 的素数，其中 q 也是素数（这样的素数 q 通常称为

索菲·热尔曼素数，并且人们猜想这类素数有无穷多个）。首先，让我们使用来自 U_p（即 $\mathbb{Z}_p$的单位群）的值对数据进行编码。选择一个由数对 $(x,\ e)$ 构成的加密密钥，其中 $x \in U_p$，且 $e \in U_{p-1}$。如果 $g \in U_p$ 是我们的明文，那么密文 定义为

$$c = (gx)^{e-1}\, g.$$

一次已知明文攻击假设我们知道 g 和 c 的值；但如果在此类攻击中，我们不得不通过对这一离散对数问题进行“暴力破解”或试乘法来求解，那么我们可能必须测试 x 的每个候选值以及 e 的每个候选值。现在，$|U_p| = p-1 = 2q$ 且 $|U_{p-1}| = q-1$，因此我们有 $2q(q-1) \sim O(p^2)$ 对 $(x,\ e)$ 需要检查；当 p 的值足够大时，问题便变得难以解决。然而，还有另一个与我们更为相关的问题，其重要性更高，下面的定理对此作了概述。

定理 1 设 G 是一个阶为偶数 n 的有限群，并且 g、$x \in G$ 和 $e \in U_n$。那么，满足 $y \in G$、$f \in U_n$，且 $(gy)^{f-1} = (gx)^{e-1}$ 的不同对 $(y$、$f)$ 的数量至少为 $T(n)$。

特别地，如果 $p = 2q+1$ 是一个安全素数且 $G = U_p$，那么当 $q \equiv 1$ 模 (4) 时，此类数对至少有 $(p-3)/4$ 个；而当 $q \equiv 3$ 模 (4)时，至少有 $(p-7)/4$ 个。

显然，上述加密方案和定理可以应用于任何合适的有限群；在第 3 节中，我们将进一步介绍其密码学背景，并概述定理 1 第一部分的证明，同时还将讨论该定理第二部分一个有趣的强化扩展。目前，我们主要关注函数 $T(n)$，因为上述定理表明，当我们遍历 $O(p^2)$ 对 (y, f)、计算 $(gy)^{f-1}$ 并将该值与 $(gx)^{e-1}$进行核对时，至少会有 $T(n)$ 个这样的数对能够匹配，但其中只有一个是“正确”的解 (x, e)。因此，显然有必要确保 $T(n)$ 相对于 n 足够大。打个比方来说，我们是在一大堆完全相同的针中寻找一根特定的针。

有关群和离散对数问题在现代密码学中的更多应用详情，请参见例如 [5]。有关初等数论中的一些基本结果和记号，请参阅该主题的任何入门读物，例如 [6]。

2 欧拉函数

我们将函数 $T\colon \mathbb{N} \to \mathbb{N}$ 定义为

$$T(n) = \left|\{1 \le m \le n \mid \gcd(m,n) = \gcd((m-1)/2, n) = 1\}\right|.$$

为完整起见，我们定义[1] $T(1) = 0$。很容易证明 T 不是乘法函数，例如 $T(2) = 0$，$T(5) = 1$（$m = 3$ 是唯一合适的单位），而 $T(10) = 2$（$m = 3$ 和 7）。此外，似乎要为 n 的所有取值计算出闭式公式相当复杂。不过，我们将设法为 n 的许多取值做到这一点，并为其他取值给出相对较小的界。

我们的欧拉函数 T 是另外两个函数的推广，并且与它们有关，其中第一个函数相当著名。欧拉函数通常记作 ϕ，它计算 $\mathbb{Z}_n$ 中单位元的数量；$\mathbb{Z}_n$ 是模 n 整数环。众所周知，ϕ 是积性的，也就是说，当 n 和 m 互素时，$\phi(n)\phi(m) = \phi(nm)$，因此很容易确定

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

其中 p 遍历 n 的所有不同的素因子。与 T 相关的第二个欧拉函数是 Schemmel [7] 于 1869 年引入的函数。Schemmel 欧拉函数 $S_r(n)$ 计算，$m+1, \ldots, m+(r-1) \leq n$ 中与 n 均互素的连续整数的数量，换言之，即 $\mathbb{Z}_n$ 中 r 个连续单位元的数量。很容易证明，这个函数也是积性的，并且

$$S_r(n) = n \prod_{p|n} \left(1 - \frac{r}{p}\right).$$

为简化记号，我们令

$$S(n) = S_2(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right),$$

又由于 S 是乘法性的，令 $S(1) = 1$ 会更方便。
值得在此指出，以备后续参考：若 $p_1, \ldots, p_\omega$ 是 $n > 1$ 的不同的素因子，则

$$S(n) = n \left(1 - \sum_{i=1}^{\omega} \frac{2^1}{p_i} + \sum_{i_1 \neq i_2} \frac{2^2}{p_{i_1} p_{i_2}} - \ldots + (-1)^\omega \sum_{i=1}^{\omega} \frac{2^\omega}{p_1 \cdots p_\omega}\right). \qquad (1)$$

我们将首先考察 $T(n)$，研究 n 为奇数的情形。

定理 2 设 p 是奇素数，$e \geq 1$ 是整数。则

$$T(p^e) = (p^e - 2p^{e-1} - 1)/2 = \frac{p^e}{2}\left(1 - \frac{2}{p} - \frac{1}{p^e}\right) = \frac{S(p^e) - 1}{2}.$$

[1] 有一种观点认为，$T(1) = 1$ 可能更合适。不过，由于我们主要关注 n 的较大取值，目前我们满足于令 $T(1) = 0$。

证明。 我们必须统计满足 $m \not\equiv 0 \bmod p$ 且$(m-1)/2 \not\equiv 0 \bmod p$的奇整数 $1 \le m \le p^e$ 。另一种做法是，统计不满足该条件的项数，再用 p^e减去它。上述条件的否定为

$$(m \equiv 0 \bmod p) \vee (m \equiv 1 \bmod 2p) \vee (m \equiv 0 \bmod 2).$$

满足第一个条件的元素有 p^{e-1} 个，满足第二个条件的有（$p^{e-1}+1$）/2 个，满足第三个条件的有（p^e-1）/2 个。然而，同时满足第一个和第三个条件的有（$p^{e-1}-1$）/2 个，因此所求的数量为

$$p^e - p^{e-1} - \frac{p^{e-1}+1}{2} - \frac{p^e-1}{2} + \frac{p^{e-1}-1}{2} = \frac{p^e - 2p^{e-1} - 1}{2}.$$

■

继续之前，我们先回顾一些基本的二项级数。设 k 为正整数，并定义

$$k' = k - \frac{1+(-1)^k}{2}, k'' = k - \frac{1-(-1)^k}{2}.$$

Then

$$\frac{3^k-1}{2} = \binom{k}{1} + 2\binom{k}{2} + \ldots + 2^{k-1}\binom{k}{k}$$

$$2^k = \binom{k}{0} + \binom{k}{1} + \binom{k}{2} + \ldots + \binom{k}{k}$$

$$2^{k-1} = \binom{k}{1} + \binom{k}{3} + \ldots + \binom{k}{k'} = \binom{k}{0} + \binom{k}{2} + \ldots + \binom{k}{k''}$$

定理 3 设 $n > 1$ 为具有 ω 个不同素因子的奇整数。则

$$\left| T(n) - \frac{S(n)-1}{2} \right| \le \frac{3^\omega - 2^{\omega+1} + 1}{2}.$$

证明。 要计算 $T(n)$，我们需要从集合 $\{1, \ldots, n\}$ 中移除满足以下条件的那些数： m 与 n 有非平凡公因子， m 是形如 $1+2m'$ 的数，其中 m' 与 n 及偶整数有非平凡公因子。换言之，移除偶整数后，对于每个满足 $q|n$ 的素数 q，我们移除形如 kq 的整数，以及当 k 为奇数、l 为偶数时的 $1+lq$。设 $p>1$ （不一定是素数）是 n 的一个奇数因子，并定义

$$B_p = \{m | 1 \le m \le n, p|m, m \text{ odd}\},$$
$$C_p = \{m | 1 \le m \le n, p|(m-1), m \text{ odd}\},$$
$$A_p = B_p \cup C_p \text{ and } A = \bigcup_{p|n} A_p.$$

注意到 $T(n) = n - (n-1)/2 - |A| = (n+1)/2 - |A|$。还应注意，$|B_p| = |C_p| = (n+p)/2p$，并且如果 $p > 1$ 和 $q > 1$ 是 n 的互素奇因子，那么 $B_p \cap B_q = B_{pq}$ 和 $C_p \cap C_q = C_{pq}$。因此，由于 $B_p \cap C_p = \emptyset$，我们得到 $|A_p| = n/p + 1$。

我们将使用容斥原理计算 $|A|$，但首先需要几个引理。

引理4 设 $p > 1$ 和 $q > 1$ 是奇正整数 n的互素奇因子。那么

$$|B_p \cap C_q| = |B_q \cap C_p| = (n \pm pq)/2pq,$$

证明。先考虑 $B_p \cap C_q$。设 $px = 1 + qy \le n$ 对于奇数 x。我们必须计算 y 为偶数时的解的个数。暂且不考虑 x 和 y的奇偶性。若 $(x_0,\ y_0)$ 是该方程组的最小非负解，则丢番图方程的通解为

$$p(x_0 + qt) = 1 + q(y_0 + pt) \tag{2}$$

对于 $t \in \mathbb{Z}$。容易得出 $x_0 < q$、$y_0 < p$ 和 $y_0 + pt \le (n-q)/q \le (n-1)/q$。注意，$p \nmid y$。若 $n \ne pq$，则将整数区间$[1, n/q - 1]$划分为子区间 $[1, p]$、$[p+1, 2p]$、$[2p+1, 3p]$、.....、$[p(n-2pq)/pq+1$、$p(n-pq)/pq]$，每个子区间中恰好包含一个满足原方程组的解 y。还要注意，这些解对应的 y值交替为偶数和奇数。因此，合并后的区间 $[1, 2p]$、$[2p+1, 4p]$、.....、$[p(n-3pq)/pq+1$、$p(n-pq)/pq]$ 各自恰好包含一个偶数解。若 $n = pq$，则不存在这样的子区间。无论哪种情况，区间的其余部分，即$[p(n-pq)/pq+1$、$n/q-1]$，也包含一个满足 y 的解；该解可能是偶数解，具体取决于最小正解 y_0是偶数还是奇数。因此，对于 y，偶数解的个数要么是 $(n-pq)/2pq$，要么是 $(n+pq)/2pq$。计算解 (x_0, y_0) 需要用到欧几里得算法，但显然，仅凭 p 和 q，并不容易确定 y_0 的奇偶性。

在计算 $B_q \cap C_p$ 时，我们考虑丢番图方程 $qx = 1 + py$，并且可以得出类似的结论。注意，在这种情况下，通解为

$$q(pt - y_0) = 1 + p(qt - x_0), \tag{3}$$

对于 $t \in \mathbb{Z}$，且 $(x_0,\ y_0)$ 是方程 (2) 的最小非负解。因此，方程 (3) 的最小非负解为 $(p - y_0,\ q - x_0)$。由于 $q - x_0$ 与 y_0 奇偶性相同，因此我们可以得出结论：$|B_p \cap C_q| = |B_q \cap C_p|$。

■

引理5 设 $p_1,\ \ldots,\ p_k$ 是 n 的 $k \ge 2$ 两两互素的奇非平凡因子。则

$$2 - 2^{k-1} + \frac{2^{k-1}n}{p_1 \ldots p_k} \le \left| \bigcap_{i=1}^{k} A_{p_i} \right| \le 2^{k-1} + \frac{2^{k-1}n}{p_1 \ldots p_k}.$$

证明。 设 $r = p_1 \dots p_k$。 注意到 $\cap_{i=1}^{k} A_{p_i} = \cap_{i=1}^{k} (B_{p_i} \cup C_{p_i})$ 。因此

$$\bigcap_{i=1}^{k} A_{p_i} = B_r \cup C_r \cup \bigcup_{p,q} (B_p \cap C_q)$$

其中， p 和 q 遍历由少于 k 个项 p_i组成的所有乘积，且 $r = pq$ 、 p 和 q 互素。

证明 B_r, C_r 以及每个 $B_p \cap C_q$ 两两不相交相对容易。注意，若 $m \in B_r \cap C_r$ ，则 $m = rx = 1 + ry$ ，因此 $r|1$。若 $m \in B_r \cap (B_p \cap C_q)$，则 $m = rx = py = 1 + qz$ ，因此 $q|1$。若$m \in C_r \cap (B_p \cap C_q)$，则 $m = 1 + rx = py = 1 + qz$ ，因此 $p|1$。现在令$m \in (B_p \cap C_q) \cap (B_q \cap C_p)$。于是 $m = px = 1 + qy = qz = 1 + pw$，因此 $p|1$。最后，若 $\{p, q\} \neq \{s, t\}$ ，且若 $r = pq = st$和 $m \in (B_p \cap C_q) \cap (B_s \cap C_t)$，则 $m = px = 1 + qy = sz = 1 + tw$。由于 $p \neq s$ ，因此存在 $p_i|p$和$p_i \nmid s$ ，由此可推得 $p_i \nmid q$ 和 $p_i|t$。因此我们可得 $p_i|1$。

因此，由前一个引理可得

$$|B_p \cap C_q| = \frac{n \pm r}{2r}$$

and

$$|C_r| = \frac{n + r}{2r}, |B_r| = \frac{n + r}{2r}.$$

于是

$$2^{k-1}\left(\frac{n}{r} - 1\right) + 2 \leq \left|\bigcap_{i=1}^{k} A_{p_i}\right| \leq 2^{k-1}\left(\frac{n}{r} + 1\right).$$

注意，由于 $|B_p \cap C_q| = |B_q \cap C_p|$ ，还可得 $\left|\bigcap_{i=1}^{k} A_{p_i}\right|$ 为偶数。

■

现在假设 p_1、.....、 p_ω 是 n 的互不相同的奇素因子。利用容斥原理，我们得到

$$|A| = |\bigcup_{i=1}^{\omega} A_{p_i}| = \sum_{\emptyset \neq K \subseteq \{1,\dots,\omega\}} (-1)^{|K|-1} \left|\bigcap_{i \in K} A_{p_i}\right|,$$

由上述论述可得 $|A|$为偶数。此外，由上文可知， $|A|$ 的一个上界为

$$\sum_{i=1}^{\omega}\left(\frac{n}{p_i} + 1\right) - \sum_{i_1 \neq i_2 \leq \omega}\left(\frac{2n}{p_{i_1}p_{i_2}} - 2^1 + 2\right) + \sum_{i_1, i_2, i_3 \text{ distinct } \leq \omega}\left(\frac{2^2 n}{p_{i_1}p_{i_2}p_{i_3}} + 2^2\right) - \dots$$

利用方程（1）和前面给出的二项级数，可将其化简为

$$\left(\frac{n - S(n)}{2}\right) + \left(\frac{3^\omega - 1}{2} - 2^\omega\right) + 2.$$

下界为

$$\sum_{i=1}^{\omega}\left(\frac{n}{p_i}+1\right)-\sum_{i_1\neq i_2\leq\omega}\left(\frac{2n}{p_{i_1}p_{i_2}}+2\right)+\sum_{i_1,i_2,i_3\text{ distinct }\leq\omega}\left(\frac{2^2n}{p_{i_1}p_{i_2}p_{i_3}}-2^2+2\right)-\dots$$

化简得

$$\left(\frac{n-S(n)}{2}\right)-\left(\frac{3^\omega-1}{2}-2^\omega\right).$$

因此可知， $T(n)$满足以下不等式

$$\left(\frac{S(n)-1}{2}\right)-\left(\frac{3^\omega-1}{2}-2^\omega+1\right)\leq T(n)\leq\left(\frac{S(n)-1}{2}\right)+\left(\frac{3^\omega-1}{2}-2^\omega+1\right).$$

至此，定理 3 的证明完成。 ■

注意，定理 2 是此结果的推论；当 $n\equiv$1 mod (4) 时， $T(n)$ 为奇数，而当 $n\equiv 3$ mod (4) 时， $T(n)$ 为偶数。

推论 6 若 $n=p^eq^f$ 满足 p 且 q 为不同素数，并且 $e,f\geq 1$ ，则

$$T(n)=\frac{S(n)-3}{2}\ or\ T(n)=\frac{S(n)+1}{2}.$$

证明。 观察到 $|B_p\cap C_q|=|B_q\cap C_p|$后，这可由定理 3 的证明推出。给定 p 和 q的具体值，似乎很难预先判断最终会出现这两个值中的哪一个。 ■

现在考虑 n为偶数的情况。首先，

定理 7 设 $e>1$ 为一个整数。则 T（2） $=0$ 并且

$$T(2^e)=2^e-3\times 2^{e-2}=2^e\left(1-\frac{3}{4}\right)=2^{e-2}.$$

证明。 如果 $e>1$ ，那么这次我们需要计数的数目是

$$(m\equiv 0\bmod 2)\vee(m\equiv 1\bmod 4).$$

有 2^{e-1} 个满足第一个条件，有 $2^{e-1}/2$ 个满足第二个条件。因此得证。 ■

定理 8 设 $n>1$ 为一个奇整数。则

$$T(2^2n)=S(n).$$

证明。 要计算 $T(4n)$，我们必须从剩余类集合$\{1,\dots,4n\}$ 中移除形式为 m 的数

1. $m = 2x$;
2. $m = xp$ 其中 $p|n, p > 1$ 且 x 为奇数;
3. $m = 1$ 或 $m = 1 + 2xp$ 其中 $p|n, p > 1$ 且 $\gcd(m, n) = 1$;
4. $m = 1 + 4x$ 其中 $\gcd(x, n) = 1$ 且 $\gcd(m, n) = 1$。

若 $1 \le m \le 2n$ 满足 (2) 或 (3)，则数 $m + 2n$也满足。若 $m = 1 + 4x$ 且 $\gcd(x, n) = \gcd(m, n) = 1$，则 $m + 2n = 3 + 4y$ 且 $\gcd(y, n) = \gcd(m + 2n, n) = 1$；若 $m = 3 + 4x$ 且 $\gcd(x, n) = \gcd(m, n) = 1$，则 $m + 2n = 1 + 4y$ 且 $\gcd(y, n) = \gcd(m + 2n, n) = 1$。因此，对于范围 $1 \le m \le 2n$ 内满足 (4) 的任意数 m，数 $m + 2n$不满足 (1)–(4)，不应将其删除。反过来，对于范围 $1 \le m \le 2n$ 内不满足 (1)–(4) 的任意数 m，数 $m + 2n$ 确实满足 (4)，应将其删除。因此，要计算 $T(4n)$，我们可以删除所有偶数、大于 $2n$ 的所有奇数，以及小于 $2n$ 且满足 (2) 或 (3) 的所有奇数。这样剩下的数就只有小于 $2n$ 且不满足 (2) 或 (3) 的奇数。

我们断言，剩余数的集合基数为 $S(n)$。接下来考虑数 $\{1, \ldots, n, n + 1, \ldots, 2n\}$，注意到要计算 $S(n)$，我们需要从 $\{1, \ldots, n\}$中移除满足以下条件的数 m： m和 $m-1$都与 n互素。于是，在集合 $\{n + 1, \ldots, 2n\}$中， $m + n$ 也具有这一性质，但奇偶性不同。因此，剩余项的总数为$2n - 2(n - S(n)) = 2S(n)$，其中一半是计算 $T(4n)$所需的奇数。

■

定理 9 设 $n > 1$ 为奇整数，且设 $e > 2$。那么

$$T(2^e n) = 2T(2^{e-1} n) = 2^{e-2} T(4n) = 2^{e-2} S(n).$$

证明。 设 $e \ge 3$，并将集合 $\{1, \ldots, 2^e n\}$ 划分为两个集合 $\{1, \ldots, 2^{e-1} n\}$和 $\{1 + 2^{e-1} n, \ldots, 2^e n\}$。对于第一个集合中每个对 $T(2^e n)$有贡献的元素 x，第二个集合中的元素 $x + 2^{e-1} n$ 也会对 $T(2^e n)$有贡献。反过来显然也成立。因此， $T(2^e n) = 2T(2^{e-1} n)$，结论现可通过对 e 的归纳及定理 8 得出。

■

最后一种情况讨论形如 $2n$ for $n > 1$ 的整数，其中 $n > 1$ 是奇正整数。我们采用与定理 3 中类似的方法。
要计算 $T(2n)$，我们必须从剩余类集合 $R = \{1, \ldots, 2n\}$ 中移除形如 m 的数

1. $m = 2x$;
2. $m = xp$ 其中 $p|n$ 且 x 为奇数;

3. $m = 1$ 或 $m = 1 + 2xp$ 其中 $p|n$ 且 $\gcd(m, n) = 1$;

4. $m = 1 + 4x$ where $\gcd(x, n) = \gcd(m, n) = 1$.

我们先计算满足 (4) 的值。通常，为了计算满足给定条件的值，我们先计算不满足该条件的值。
设 $n > 1$ 为奇正整数， $p > 1$ 为 n 的奇数因子。定义

$$D_p = \{m|1 \le m \le 2n, 4|(m-1) \text{ and } p|m\},$$
$$E_p = \{m|1 \le m \le 2n, 4|(m-1) \text{ and } p|(m-1)\},$$
$$F_p = D_p \cup E_p.$$

引理10 如果 $p > 1$ 是 n 的奇数因子，那么

$$|E_p| = \frac{n-p}{2p}, |D_p| = \frac{n \pm p}{2p}$$

因此

$$|F_p| = \frac{n}{p} \ or \ |F_p| = \frac{n}{p} - 1.$$

证明。 设 $n > 1$ 为奇数， $p > 1$ 为 n 的奇数因子。

1. 假设对于正整数 x 和 y， $1 + 4x = 1 + py \le 2n$ 。那么 $y \le (2n-1)/p$ 同余于 0（模 4），因此 y 有 $(2n-2p)/4p = (n-p)/2p$ 个不同的候选值。因此 $|E_p| = (n-p)/2p$。

2. 现在假设对于正整数 x 和 y， $1+4x = py \le 2n$ 。那么 $py \le 2n$ ，且 py 模 4 同余于 1。假设 $p \equiv 1$ 模 (4)。那么方程 $1+4x = py$ 的通解为 $1+4(x_0+pt) = p(1+4t)$，其中 $p = 1 + 4x_0$ 且 $t \in \mathbb{Z}$。因此 $1 + 4t \le (2n-p)/p$ ，从而 $0 \le t \le (2n-2p)/4p = (n-p)/2p$。因此，在这种情况下有 $(n+p)/2p$ 个解。

   另一方面，如果 $p \equiv 3$ 模 (4)，那么通解为 $1+4(x_0+pt) = p(3+4t)$，其中 $3p = 1+4x_0$，因此 $0 \le 4t \le 2n/p - 6$，且在这种情况下有 $(n-3p)/2p + 1 = (n-p)/2p$ 个解。
   因此 $|D_p| = (n \pm p)/2p$。

因此，对于每个 p， F_p 中要么有 n/p 个元素，要么有 $n/p - 1$ 个元素。 ■

注意，如果 $p > 1$ 和 $q > 1$ 是 n 的互素且不同的奇数因子，那么 $D_{pq} = D_p \cap D_q$ 和 $E_{pq} = E_p \cap E_q$。

引理 11 设 $p>1$ 和 $q>1$ 是 n的互素奇因子。那么

$$\frac{2n}{pq}-2\le|F_p\cap F_q|\le\frac{2n}{pq}+1.$$

证明。如果 $m\in F_p\cap F_q=D_{pq}\cup E_{pq}\cup(D_q\cap E_p)\cup(D_p\cap E_q)$，那么有 4 种可能

1. 对于适当的 $x,y,z\in\mathbb{N}$，有 $1+4z=px=qy\le 2n$。于是 $1+4z\in D_{pq}$，因此有
$$|D_p\cap D_q|=|D_{pq}|=\frac{n\pm pq}{2pq}$$
个解。

2. $1+4z=1+px=1+qy\le 2n$。于是 $1+4z\in E_{pq}$，因此
$$|E_p\cap E_q|=|E_{pq}|=\frac{n-pq}{2pq}.$$

3. $1+4z=1+px=qy\le 2n$。由上可知，$1+4z=1+px\le 2n$ 的解为：当 $1\le t\le(n-p)/2p$ 时，$z=tp$。
因此我们必须求解 $1+4pt=qy$，其中 $1\le t\le(n-p)/2p$。如果 t_0,y_0 是最小解，那么通解为
$$1+4pt_0+4pqs=qy_0+4pqs$$
对于 $s\in\mathbb{Z}$。这意味着 $t_0\le q$，因此区间 $[1,(n-p)/2p]$ 可以分成 $(n-pq)/2pq$ 个由 q 个连续整数构成的“区块”，并剩下 $(n-p)/2p-(n-pq)/2p=(q-1)/2$ 个整数。每个由 q 个整数构成的区块恰好包含一个 t 的解，因此解的数量为 $(n-pq)/2pq$ 或 $(n-pq)/2pq+1=(n+pq)/2pq$。因此
$$|E_p\cap D_q|=\frac{n\pm pq}{2pq}.$$
注意，如果 $pq=n$，那么就没有由 q 个整数构成的“区块”，但剩下的 $(q-1)/2$ 个整数中仍可能有一个解。

4. $1+4z=1+qy=px\le 2n$。根据对称性，解的数量为 $(n-pq)/2pq$ 或 $(n+pq)/2pq$。因此
$$|D_p\cap E_q|=\frac{n\pm pq}{2pq}.$$

因此得到该结果。 ■

引理 12 设 $p_1, \ldots, p_k$ 是 $k \geq 2$ 两两互素的奇数非平凡因子，且它们整除 n。那么

$$-2^{k-1} + \frac{2^{k-1}n}{p_1 \ldots p_k} \leq \left| \bigcap_{i=1}^{k} F_{p_i} \right| \leq 2^{k-1} - 1 + \frac{2^{k-1}n}{p_1 \ldots p_k}.$$

证明。 令 $r = p_1 \ldots p_k$。 注意 $\cap_{i=1}^{k} F_{p_i} = \cap_{i=1}^{k} (D_{p_i} \cup E_{p_i})$。因此

$$\bigcap_{i=1}^{k} F_{p_i} = D_r \cup E_r \cup \bigcup_{p,q} (D_p \cap E_q)$$

其中 p 和 q 遍历由少于 k 个项 p_i 的乘积，且 $r = pq$ 与 p 互素， q 与它们互素。根据前一个引理，我们有

$$|D_p \cap E_q| = \frac{n \pm r}{2r}$$

and

$$|E_r| = \frac{n - r}{2r}, |D_r| = \frac{n \pm r}{2r}.$$

因此

$$\frac{2^k}{2}\left(\frac{n}{r} - 1\right) \leq \left| \bigcap_{i=1}^{k} F_{p_i} \right| \leq \frac{2^k - 2}{2}\left(\frac{n}{r} + 1\right) + \frac{n}{r}.$$

■

假设 n 有 ω 个互不相同的奇素因子 $p_1, \ldots, p_\omega$。由于集合 $\{1, \ldots, 2n\}$ 中有 $(2n-2)/4 = (n-1)/2$ 个值模 4 同余于 1，排除 1 后，还有

$$\frac{n-1}{2} - \left| \bigcup_{i=1}^{\omega} F_{p_i} \right|$$

个值 m，排除 1 后，它们模 4 同余于 1，但 m 和 $m-1$ 都没有与 n 公因子。利用容斥原理可知，这个数量至多为

$$\frac{n-1}{2} - \sum \left(\frac{n}{p_i} - 1\right) + \sum \left(\frac{2n}{p_i p_j} + 1\right) - \ldots$$

利用方程（1），可简化为

$$-\frac{1}{2} + \frac{n}{2} \prod_{i=1}^{\omega} \left(1 - \frac{2}{p_i}\right) + \omega + (2^1 - 1)\binom{\omega}{2} + 2^2\binom{\omega}{3} + (2^3 - 1)\binom{\omega}{4} + \ldots$$

因此，上界为

$$\frac{1}{2}\left(S(n)-1\right)+\omega+2^1\binom{\omega}{2}+2^2\binom{\omega}{3}+2^3\binom{\omega}{4}+\ldots-\binom{\omega}{2}-\binom{\omega}{4}-\ldots$$

or

$$\frac{1}{2}\left(S(n)-1\right)+\frac{1}{2}3^\omega-\frac{1}{2}-\frac{1}{2}\left(2^\omega-2\right)=\frac{1}{2}\left(S(n)+3^\omega-2^\omega\right).$$

下界为

$$\frac{n-1}{2}-\sum\left(\frac{n}{p_i}\right)+\sum\left(\frac{2n}{p_ip_j}-2\right)-\ldots$$

化简得

$$\frac{1}{2}\left(S(n)-1\right)-\frac{1}{2}\left(2^2\binom{\omega}{2}+2^3\binom{\omega}{3}+2^4\binom{\omega}{4}+\ldots\right)+\binom{\omega}{3}+\binom{\omega}{5}+\ldots$$

or

$$\frac{1}{2}\left(S(n)-1\right)-\frac{1}{2}\left(3^\omega-2\omega-1\right)+\frac{1}{2}\left(2^\omega-2\omega\right)=\frac{1}{2}\left(S(n)-\left(3^\omega-2^\omega\right)\right).$$

定理13 设 $n>1$ 是一个具有 ω 个不同素因子的奇整数。则

$$\left|T(2n)-\frac{S(n)-1}{2}\right|\leq\frac{3^\omega-2^\omega+1}{2}.$$

若 $n=p^e$，其中 p 是素数且 $e>0$，则 $T(2n)=(S(n)-1)/2$ 当 $p\equiv 3$ 模 (4) 时，以及 $T(2n)=(S(n)+1)/2$ 当 $p\equiv 1$ 模 (4)时。

证明。回想一下，要计算 $T(2n)$，我们需要从剩余类集合 $R=\{1,\ldots,2n\}$ 中去除形如以下形式的数：

1. $m=2x$;
2. $m=xp$ 其中 $p|n$ 且 x 为奇数;
3. $m=1$ 或 $m=1+2xp$，其中 $p|n$ 且 $\gcd(m,n)=1$;
4. $m=1+4x$ 其中 $\gcd(x,n)=\gcd(m,n)=1$。

将集合 R 划分为 n 个不相交子集 $R_i=\{i,n+i\}$，其中 $1\leq i\leq n$。找出满足以下条件的集合 R_j：要么 $j=1$，$\gcd(j,n)\neq 1$，要么 $\gcd(j-1,n)\neq 1$。这样的子集有 $n-S(n)$ 个。若 j 为奇数，则 j 满足条件 (2) 或 (3)。若 j 为偶数，则 $n+j$ 满足条件 (2) 或 (3)。因此，R_j 中的所有元素都满足条件 (1)、(2) 或 (3)，应予以移除。对于剩余子集 R_k，一半元素为偶数，另一半为奇数，且不满足条件 (1)、(2) 或 (3)。因此有 $S(n)$ 个这样的

奇数项，其中一些可能满足条件 (4)。由上可知，这些满足条件 (4) 的项有 $S(n)$ 个，其数量范围为

$$\left[\frac{1}{2}\left(S(n)-(3^{\omega}-2^{\omega})\right),\frac{1}{2}\left(S(n)+(3^{\omega}-2^{\omega})\right)\right]$$

因此， $T(2n)$ 位于值域内

$$\left[\frac{1}{2}\left(S(n)-(3^{\omega}-2^{\omega})\right),\frac{1}{2}\left(S(n)+(3^{\omega}-2^{\omega})\right)\right].$$

最后一部分由引理10（的证明）得出。 ■

总而言之，若 $n=2^{e}m$ 对于 $e\geq 0$，且 $m>1$ 为奇数，并且 ω 是 m 的不同素因子个数，则

1. $T(1)=T(2)=0$ 且 $T(2^{e})=2^{e-2}$ 对于 $e\geq 2$;
2. $T(n)=2^{e-2}S(m)$ 对于 $e\geq 2$; 3. $\left|T(n)-{}^{S}{}_{(m)}{}_{2}{}^{-1}\right|\leq(3^{\omega}-2^{\omega}+1)/2$ 对于 $e=1$; 4. $\left|T(n)-{}^{S}{}_{(m)}{}_{2}{}^{-1}\right|\leq\overline{(3^{\omega}-2^{\omega+1}+1)/2}$ 当 $e=0$ 时;

5. $T(n)=(S(m)-1)/2$ 如果 $e=1$ 和 $m=p^{f}$， $f>0$ 其中 $p\equiv 3$ 模 4 是素数;
6. $T(n)=(S(m)-1)/2+1$ 如果 $e=1$ 和 $m=p^{f}$， $f>0$ 其中 $p\equiv 1$ 模 4 是素数;
7. $T(n)=(S(m)-1)/2$ 当 $e=0$ 和 $\omega=1$;
8. $T(n)=(S(m)-1)/2\pm 1$ 当 $e=0$ 和 $\omega=2$。

3 离散对数与群的变体

本节将更详细地介绍第 1 节中提到的密码方案；该方案正是我们引入欧拉函数 $T(n)$ 的动机。

设 G 为阶为 n 的有限群。如果 $g\in G$ 且 $e\in U_{n}$，那么存在 $e'\in U_{n}$，使得 $ee'\equiv 1 \mod n$，因此

$$g=g^{ee'}=(g^{e})^{e'}.$$

在密码学术语中，我们将 g 称为明文，将 e称为密钥，将 g^{e}称为密文。我们还将 e称为 g^{e} 的离散对数模 g。

离散对数问题是指已知 g 和 g^e，求出 e的问题。许多密码系统都依赖于某些合适的群 G中该问题难以求解这一性质。

如果我们只能通过暴力破解来解决离散对数问题，那么就可能必须测试集合 U_n 中每个候选值 e。根据定义， $|U_n| = \phi(n)$；如果我们谨慎选择群，就可以预期 $\phi(n) \sim O(n)$，因此当 n 的值足够大时，这个问题将变得不可行。

另一种略有不同且可能提高安全性的方法，是使用群的一个变体。Hickey [3, 4]，在 Chase [1, 2]，早期关于二元关系半群变体的研究基础上，在半群理论中引入了变体；此后，人们研究了半群变体的许多有趣性质和类型。如果 $(S, \cdot)$ 是一个半群，且 $s \in S$ ，那么我们可以在 S 上定义一种新的乘法 $*_s$，如下所示：

$$x *_s y = x \cdot s \cdot y.$$

容易验证，这定义了一个结合运算，因此系统 $(S, *_s)$ 是一个半群，称为 S 的变体，通常记作 S^s。群只是一种特殊的半群；如果 $(G, \cdot)$ 是一个群，且 $x \in G$ ，那么容易验证系统 $G^x = (G, *_x)$ 也是一个群，其单位元为 x^{-1} ，而 g 在 G^x 中的逆元由 G 中的元素 $x^{-1} \cdot g^{-1} \cdot x^{-1}$ 给出；其中 x^{-1} 和 g^{-1} 分别是基群 $(G, \cdot)$ 中 x 和 g 的逆元。也容易看出，由 $g \mapsto g \cdot x^{-1}$ 给出的映射 $(G, \cdot) \to (G, *_x)$ 是一个群同构（半群中通常并非如此）。显然，如果 $e \in \mathbb{N}$ ，那么在 G^x 中，元素 g^e（即元素 g 的 e^{th} 次幂）由 $(g \cdot x)^{e-1} \cdot g$ 在 $(G, \cdot)$ 中表示。为简化记法，以下省略符号“$\cdot$”，并将其写作 $(gx)^{e-1} g$。

因此，变体 G^x 中的离散对数问题，就是在已知 g 和 $c = (gx)^{e-1} g$的情况下求出 e的问题。然而，如果 x 被保密，那么这就不同于标准情形（如果已知 x，我们就能计算出 gx 和 $(gx)^e$ ，从而将问题化归为“标准”离散对数问题）。因此，思路是使用数对 $(x,\ e)$作为密钥，将 g 加密 为 $(gx)^{e-1} g$。收到密文的一方可以先使用欧几里得算法计算出 $e' \in U_n$ ，使得 $ee' \equiv 1 \mod (n)$，然后计算

$$(cx)^{e'} x^{-1} = \left((gx)^{e-1} gx\right)^{e'} x^{-1} = (gx)^{ee'} x^{-1} = gxx^{-1} = g.$$

如果攻击者除了 g 和 c之外没有其他信息，那么针对这个离散对数问题进行“暴力破解”攻击，就需要计算所有形如 $(gy)^{f-1}$的值，其中 y 遍历 G 中的所有值，而 f 遍历 U_n中的所有值。因此，这样的数对共有 $n\phi(n) \sim O(n^2)$ 个，实际上使安全性翻倍。

然而，还有另一个需要考虑的问题：是否会出现“假阳性”。换句话说，是否可能存在 $(gx)^{e-1} = (gy)^{f-1}$，使得 $(x,\ e) \neq (y,\ f)$？我们可以将这个问题转化如下。给定一个阶为 n 的有限群 G 和一个固定（常数）元素$c \in G$，我们希望求出 $\mathbb{Z}_n$中的单位元 $f > 1$ 的个数，使其满足方程

$$w^{f-1} = c \tag{4}$$

已知至少存在一组 f 和 w 的值使该方程成立，则 G 中存在一个解。

定理 14 设 G 是一个阶为 n 的有限群，c 是 G 中的固定常数，并假设对于至少一个 f 的取值，方程 *4* 有解。若 n 为奇数，则方程 *4* 至少有 $S(n)$ 个解；若 n 为偶数，则至少有 $T(n)$ 个解。

证明。设 n 为奇数，并设 $f-1$ 也是 $\mathbb{Z}_n$ 中的一个单位元，其逆元为 k。则 $w = c^k$ 是一个解，因为 $\left(c^k\right)^{f-1} = c$。根据定义，$\mathbb{Z}_n$ 中有 $S(n)$ 个这样的单位元。
另一方面，若 n 为偶数，则 f 必为奇数，因此，若存在解，则对于某个 $h \in G$，有 $c = h^2$。在这种情况下，设 $(f-1)/2$ 也是 $\mathbb{Z}_n$ 中的一个单位元，其逆元为 k。则 $w = h^k$ 是方程（4）的一个解，因为

$$\left(h^k\right)^{f-1} = \left(h^k\right)^{2(f-1)/2} = \left(h^2\right)^{k(f-1)/2} = h^2 = c.$$

因此，至少有 $T(n)$ 个这样的解。 ■

因此，利用群变体，我们可以有效地将针对离散对数问题的简单暴力攻击的安全性提高一倍；同时，通过选择足够大的 n，使 $S(n)$ 和 $T(n)$ 足够大，就能让密钥难以被发现。

对于我们在第 1 节中给出的具体示例，情况甚至更加有趣。

命题 15 若 $G = U_p$，其中 $p = 2q+1$ 是一个安全素数，则方程 *4* 有$p-5 = 2(q-2)$ 个解。

证明。由定理 14 可知，每个满足以下性质的单位 $f > 1$：$(f-1)/2$ 也是单位，都提供了一个解，记作 w。注意，在这种情况下，$-w$ 也是一个解。如果 $(f-1)/2$ 不是单位，那是因为它是偶数；此时 $(f-1)/4$ 可能是单位。若不是，那么 $(f-1)/4$ 是偶数，因此 $(f-1)/8$ 可能是单位。如此继续下去，我们可以看出，存在一个正整数 m，使得 $(f-1)/2^m$ 是单位。
众所周知，如果 $p \equiv 3 \bmod(4)$ 是素数，那么 $y \in \mathbb{Z}_p$ 时，y 或 $-y$（但不能两者同时）在模 p 下有平方根（该平方根

实际上是 $y^{(p+1)/4}$ 。如果在方程 4 中， $c = h^2$ ，那么 h 或 $-h$ 将有一个平方根， h_1 ，因此 $c = h_1^4$。但这样一来， h_1 或 $-h_1$ 将有一个平方根， h_2 ，因此 $c = h_2^8$。照此继续，我们可知$c = h_{m-1}^{2^m}$。所以，如果 k 是 $(f-1)/2^m$ 的乘法逆元，那么 $w = \pm h_{m-1}^k$将是方程 4 的解。因此，在 $\mathbb{Z}_p$ 中，每个单位 $f > 1$ 都会提供两个解；又由于 $|U_{p-1}| = q - 1$ ，结论得证。 ■

实际上，存在某些已知明文攻击，有时可以将这个离散对数问题简化为更经典的情形；而为每次加密随机选择一个 x 将有助于缓解这一问题。例如，选择 $e \in U_n$ 和 $s \in \mathbb{Z}_m$ ，其中 $m \geq n$ ，并令数对 (s, e) 为密钥。给定明文 $g \in G$ 后，令 i 为 $\mathbb{Z}_m$ 中的一个随机值，并定义 $x_i = H(i \oplus s)$，其中 $\oplus$ 是按位异或运算符， H 是一个经过适当选择的密码哈希函数，其像与 G 重合。于是，密文就是数对 $(i, (gx_i)^{e-1}g)$；任何能够访问密钥的人都可以复现 x_i ，并像之前一样进行解密。然而，即使攻击者能够从定理 14 中的所有 $T(n)$ 个或更多个数对中识别出 x_i 的正确值，这也将相对无效，因为我们会为每次加密使用不同的 x_i 值。

注意，如果对于某个 $r > 1$ ，$(m-1)$ 能被 r 整除，那么具有性质 $s = (m-1)/r$ 的单位 $m = 1 + rs$ 也可能为我们提供方程（4）的一个不同解。这表明，研究计算满足 $(m-1)/r \in U_n$ 的单位 $m \in U_n$ 个数的函数 $T_r(n)$，或许也会有所助益。

最后，考虑到引理4的证明，我们可以考虑下面这个问题。若 p 和 q 是互素的奇正整数，那么利用欧几里得算法可以找到正整数 a 和 b ，使得 $ap - bq = 1$，并且 a 和 b 是满足条件的最小正整数。我们很容易看出， a 和 b 的奇偶性必然不同。给定这样的 p 和 q，我们能否预测 a 和 b 中哪一个是偶数?

参考文献

[1] Karen Chase，二元关系的夹心半群，*Discrete Math.*，28（1979），231-236。[2] Karen Chase，二元关系的新半群，*Semigroup Forum*，18（1979），79-82。[3] J. B. Hickey，夹心运算下的半群，*Proc. EdinburghMath. Soc.*，26（1983），371-382。[4] J.B. Hickey，半群的变体，*Bulletin of the AustralianMathematical Society*，第34卷，第3期，（1986），447–459。

[5] Jeffrey Hoffstein、Jill Catherine Pipher 和 Joseph H. Silverman，《数学密码学导论》，（施普林格，2014）[6]Gareth A. Jones 和 J. Mary Jones，《初等数论》，施普林格本科数学丛书，（施普林格，2005）。.[7] Schemmel, V. 关于相对素数，Journal für die reine und angewandte Mathematik，第70卷（1869），第191–192页。