详细解答

STEP II 1994，第 1 题

纯数学 · 整除性与十进制数字

> **STEP II 1994，第 1 题**
>
> 继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：
>
> step.maths.org/questions/94-s2-q1

关键思路

乘积的最后几位数字,只取决于各因数的最后几位数字,所以本题的一切运算都是模(modulo）10 的某个幂的算术。末位为 1、3、7 或 9 的数与 10 没有公因数，因此它在模 10 之下是可逆（invertible）的，事实上在模 10 的任何幂之下也是可逆的。中间部分把 2 和 5 这些因数从 n 中抽出来，再把它们变成零。最后部分则利用模 10^{10} 之下的可逆性，迫使乘积的最后十位数字成为我们想要的任何一组数字。

解答

第 1 部分：末位为 1 的倍数

$n \times m$ 的末位数字，就是（n 的末位数字）×（m 的末位数字）的末位数字，因为其余各位数字只会贡献 10 的倍数。由于 n 的末位既不是 5 也不是偶数，所以它的末位是 1、3、7 或 9，而

$$1 \times 1 = 1, \qquad 3 \times 7 = 21, \qquad 7 \times 3 = 21, \qquad 9 \times 9 = 81.$$

因此分别取 $m = 1$、7、3 或 9 即可。这样 $n \times m$ 的末位便是 1，正如所求。

第 2 部分：任意的 n

写成

$$n = 2^a 5^b k,$$

其中 $a, b \geq 0$，而 k 既不能被 2 整除，也不能被 5 整除。于是 k 的末位既不是 5 也不是偶数，所以由第 1 部分可知，存在 m' 使得 km' 的末位是 1。现在设

$$m = 2^b 5^a m'.$$

那么

$$n \times m = 2^{a+b} 5^{a+b} km' = 10^{a+b} (km').$$

乘以 10^{a+b} 只不过是在 km' 之后添上 $a+b$ 个零。所以，若 $a+b=0$，则 $n \times m$ 的末位是 1；否则它的结尾是 1 后面跟着 $a+b$ 个零。这正是我们所需要的。

例如，$n = 40 = 2^3 \cdot 5$ 对应 $k=1$，所以 $m = 2 \cdot 5^3 = 250$，而 $n \times m = 10\,000$。

第 3 部分：齐集十个数字

写成 $n = 10^r q$，其中 $r \geq 0$，而 q 的末位是 1。在末尾添零不会令任何数字消失，所以只需找出 m，使 $q \times m$ 包含每一个数字；这样 $n \times m = 10^r (qm)$ 也会包含它们。

设 $N = 10^{10}$ 及 $X = 1234567890$，后者包含每一个数字。我们的目标是

$$qm \equiv X \pmod{N},$$

也就是说，qm 的最后十位数字是 1234567890。

> **想一想** 为甚么 q 必定有某个倍数，除以 10^{10} 时余数（remainder）是 X?

考虑 N 个数 $q \times 0$, $q \times 1$, …, $q \times (N-1)$，以及它们模 N 的余数。假设其中两个余数相等，譬如 $qs \equiv qt \pmod{N}$，其中 $0 \leq t < s \leq N-1$。那么 10^{10} 整除 $q(s-t)$。但 q 的末位是 1，所以它是奇数，也不是 5 的倍数，因而与 $10^{10} = 2^{10}5^{10}$ 没有公共的质因数。由此可知 $2^{10}5^{10}$ 整除 $s-t$，但这是不可能的，因为 $0 < s-t < N$。所以这 N 个余数各不相同。可能出现的余数只有 N 个，即 $0, 1, \ldots, N-1$，所以每一个都会出现。特别地，存在某个满足 $0 \leq m \leq N-1$ 的 m，使得 $qm \equiv X \pmod{N}$。

这个 m 不是 0，因为 $X \neq 0$。所以 qm 是一个正的倍数，且 $qm \geq X \geq 10^9$。因此它的最后十位数字正好是 $1, 2, 3, 4, 5, 6, 7, 8, 9, 0$，而 X 开首的 1 也确实存在。于是 $q \times m$ 包含 $0, 1, \ldots, 9$ 所有数字，$n \times m$ 亦然。

举例来说，当 $n = 21$ 时，我们可以取 $m = 7\,201\,646\,090$，这时 $21 \times m = 151\,234\,567\,890$。

> **想一想** 关于 n 的假设在哪里用过？为甚么需要它?

我们用它只是为了知道 q 没有因数 2 或 5。没有这一点，余数 $qm \bmod 10^{10}$ 就不能取遍所有的值。例如，2 的每个倍数都是偶数，所以结尾不可能是 …1。正是这个假设让我们可以指定乘积的结尾。（第 2 部分证明了任意的 n 都有一个这种形式的倍数，所以与第 3 部分结合起来，每一个 n 都有一个包含全部十个数字的倍数。）

验算

- 用手验算第 1 部分：$13 \times 7 = 91$ 及 $29 \times 9 = 261$。
- 电脑验算证实，第 1 部分的方法对每一个末位既不是 5 也不是偶数的 $n \leq 20\,000$ 都成立。它亦证实第 2 部分的构造对每一个 $n \leq 20\,000$，以及 20 000 个不超过 10^{15} 的随机 n 都成立。它还为超过 10 000 个符合所需形式的 n 值计算了第 3 部分的乘数，当中包括末尾有好几个零的数，而在每一个情况下 $n \times m$ 都包含全部十个数字。例子：$21 \times 7\,201\,646\,090 = 151\,234\,567\,890$ 及 $11 \times 4\,657\,687\,990 = 51\,234\,567\,890$。

常见错误

- 在第 3 部分，忘记检查 1234567890 这组数字是否真的完整出现。开首的 1 需要 $qm \geq 10^9$，而这是成立的，因为 $qm \equiv X$ 且 $qm > 0$。
- 在第 2 部分，乘以 10^{a+b} 而不是 $2^b 5^a$。这样做虽然添了零，但 2 和 5 这些原本已在 n 之中的因数却原封不动。

STEP 之外

第 3 部分的鸽巢原理（pigeonhole principle）论证，其实证明了一个一般的事实：若 $\gcd(q, N) = 1$，则 q 在模 N 之下有乘法逆元（multiplicative inverse）。可逆的剩余（residue）构成一个群（group），记作 $(\mathbb{Z}/N\mathbb{Z})^\times$，这是初等数论和 RSA 密码学的起点。另一个技巧可以证明，最后部分对任何 n 都成立：只要 $10^k \geq n$，就有 n 的某个倍数介乎 $X \cdot 10^k$ 与 $X \cdot 10^k + 10^k$ 之间，而这样的倍数是以 1234567890 开首的。Davenport 的 *The Higher Arithmetic* 是一本介绍同余（congruence）与剩余的优秀入门书。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。