第九章 同余式、幂与费马小定理

> **费马小定理**：设p是素数，a是任意整数且$a \not\equiv 0 \pmod{p}$，则
> $$a^{p-1} \equiv 1 \pmod{p}$$

> **习题**

- *9.1* 利用费马小定理求解下述题目。
  - *(a)* 求数$0 \le a < 73$，使得$a \equiv 9^{794} \pmod{73}$
  - *(b)* 解$x^{86} \equiv 6 \pmod{29}$
  - *(c)* 解$x^{39} \equiv 3 \pmod{13}$

  (a) 利用 $9^{72} \equiv 1 \pmod{73}$，因为 $794 = 11 \times 72 + 2$，所以 $9^{794} = 9^{11 \times 72 + 2} = (9^{72})^{11} \cdot 9^2$
  $(9^{72})^{11} \cdot 9^2 \equiv 9^2 \equiv 8 \pmod{73}$，所以 $a = 8$
  (b) 因为29是素数且 $x \not\equiv 0 \pmod{29}$，则 $x^{28} \equiv 1 \pmod{29}$
  因为 $86 = 3 \times 28 + 2$，所以 $x^{86} = (x^{28})^3 \cdot x^2 \equiv x^2 \pmod{29}$
  即将原式转化为解 $x^2 \equiv 6 \pmod{29}$，解得 $x = 8$ 或 21
  (c) 因为13是素数且 $x \not\equiv 0 \pmod{13}$，则 $x^{12} \equiv 1 \pmod{13}$
  因为 $39 = 3 \times 12 + 3$，所以 $x^{39} = (x^{12})^3 \cdot x^3 \equiv x^3 \pmod{13}$
  即将原式转化为解 $x^3 \equiv 3 \pmod{13}$，无解

- *9.2* 虽然我们不需要知道$(p-1)! \pmod{p}$ 的值，但是$(p-1)! \pmod{p}$出现在费马小定理的证明中。
  - *(a)* 对某些小的p值，计算$(p-1)! \pmod{p}$，找出模式并提出猜想。
  - *(b)* 证明你的猜想是正确的。

  (a) $p=2$时，$(2-1)! \equiv 1 \pmod{2}$
  $p=3$时，$(3-1)! \equiv 2 \pmod{3}$
  $p=5$时，$(5-1)! \equiv 4 \pmod{5}$
  $p=7$时，$(7-1)! \equiv 6 \pmod{7}$
  $p=11$时，$(11-1)! \equiv 10 \pmod{11}$
  猜测 $(p-1)! \equiv -1 \pmod{p}$
  (b) 在模p下每个数 $1, 2, \ldots, p-1$ 都有个唯一的乘法逆元
  对于 $a \in \{1, 2, \ldots, p-1\}$，如果 $a \neq a^{-1} \pmod{p}$，则a和a^{-1}可以配对，使得 $a a^{-1} \equiv 1 \pmod{p}$
  因此，可以将$(p-1)!$分解为配对的乘积：$(p-1)! \equiv 1 \times 1 \times 1 \times \cdots \times 1 \times (p-1) \pmod{p}$
  得证

- *9.3* 当p是素数时，习题9.2要求你确定$(p-1)! \pmod{p}$的值。
  - *(a)* 对某些小的合数m的值，计算$(m-1)! \pmod{m}$。你能得到对素数所发现的相同模式吗?

- *(b)* 如果已知$(n-1)! \pmod{n}$的值，如何使用这个值明确判断n是素数还是合数？

(a) $m=4$时，$(m-1)! \equiv 2 \pmod 4$

$m=6$时，$(m-1)! \equiv 0 \pmod 6$

$m=8$时，$(m-1)! \equiv 0 \pmod 8$

$m=9$时，$(m-1)! \equiv 0 \pmod{10}$

$m=10$时，$(m-1)! \equiv 0 \pmod{12}$

推测当$m>6$时，$(m-1)! \equiv 0 \pmod m$

(b) 如果$(n-1)! \pmod n$的值为-1，那么这个值n是素数，如果$(n-1)! \pmod n$的值为0或2，那么这个数是合数

- *9.4* 如果p是素数，$a \not\equiv 0 \pmod{p}$，则由费马小定理可知$a^{p-1} \equiv 1 \pmod{p}$。
  - *(a)* 同余式$7^{1734250} \equiv 1660565 \pmod{1734251}$成立。你能得到1734251是合数的结论吗？
  - *(b)* 同余式$129^{64026} \equiv 15179 \pmod{64027}$。你能得到64027是合数的结论吗？
  - *(c)* 同余式$2^{52632} \equiv 1 \pmod{52633}$。你能得到52633是合数的结论吗？

(a) 能得到，因为如果1734251是素数，那么根据费马小定理 $7^{1734250} \equiv 1 \pmod{1734251}$

(b) 能得到，因为如果64027是素数，那么根据费马小定理 $129^{64026} \equiv 1 \pmod{64027}$

(c) 不能，因为费马小定理是单向的，只能通过不满足条件证明合数，不能通过满足条件证明素数。