信息安全数学基础 第六次作业

BY 18340087 李晨曦

(3)

我们有

$$3^{90} \equiv 1 \pmod{91}$$

但是

$$91 = 7 \times 13$$

是一个合数。所以91是基3的伪素数

(6)

由于课上没有介绍， 我们这里首先证明一下Korselt定理：

定理 1. 一个合数是*Carmichael*数， 当且仅当对其每一个素因子p都有：

1. $p^2 \nmid n$
2. $p-1 | n-1$

证明.

充分性：

如果一个合数n是Carmichael数， 那么， 对任意与n互素的b， 都有：

$$b^{n-1} \equiv 1 \pmod{n}$$

将n分解为

$$p_1^{k_1} \dots p_i^{k_i} \dots p_t^{k_t}$$

我们有：

$$b^{n-1} \equiv 1 \pmod{p_i^{k_i}}$$

所以

$$\mathrm{Ord}_{p_i^{k_i}}(b) | n-1$$

由原根的存在性， 对任意的i存在一个$p_i^{k_i}$与互素的b_i， 使得b_i是模$p_i^{k_i}$的原根。

任取$b_1 \dots b_j \dots b_n (j \neq i)$， 使得$b_j$与$p_i^{k_i}$互素， 那么，

$$\begin{aligned} b &\equiv b_1 \pmod{p_1^{k_1}} \\ &\dots \\ b &\equiv b_i \pmod{p_i^{k_i}} \\ &\dots \\ b &\equiv b_n \pmod{p_t^{k_t}} \end{aligned}$$

这个方程组是有解的， 且它的解b满足对任意的$p_j^{k_j}$，b与$p_j^{k_j}$互素。这样一来，b与n互素， 且：

$$\begin{aligned}\mathrm{Ord}_{p_i^{k_i}}(b) &= \varphi(p_i^{k_i}) \\ &= p_i^{k_i} - p_i^{k_i-1} \\ &= p_i^{k_i-1}(p-1)\end{aligned}$$

这也就是说

$$p_i^{k_i-1}(p-1)|n-1$$

因为$(p_i^{k_i-1}, p-1) = 1$， 那么必有：

$$p_i^{k_i-1} \mid n-1 \quad (1)$$
$$p_i - 1 \mid n-1 \quad (2)$$

因为$(n, n-1) = 1$， 当$k_i > 1$时 ， (1)式是不可能满足的。这也一来就证明了充分性。

必要性：

如果对n的每一个素因子p都有：

$$p^2 \nmid n$$

那么n必定是素数一次方的乘积， 也就是：

$$n = p_1 p_2 p_3 \ldots p_t$$

由于

$$\begin{aligned}p_i - 1 &\mid n-1 \\ \varphi(p) &= p_i - 1 \\ \mathrm{Ord}_p(b) &\mid \varphi(p_i)\end{aligned}$$

所以

$$\mathrm{Ord}_{p_i}(b)|n-1$$

所以

$$b^{n-1} \equiv 1 (\bmod p_i)$$

对任意与n互质的b、 任意$1 \leqslant i \leqslant t$成立， 这样一来

$$b^{n-1} \equiv 1 \pmod n$$

证明了必要性。 □

根据这个定理， 我们可以证明$2821 = 7 \times 13 \times 31$是Carmichael数：

$$\begin{aligned}6 &\mid 2820 \\ 12 &\mid 2820 \\ 30 &\mid 2820\end{aligned}$$

(10)

首先，

$$1373653 = 829 \times 1657$$

这是一个合数。

然后， 我们有：

$$1373652 = 2^2 \times 343413$$

$$\begin{aligned} 2^{2 \times 343413} &\equiv -1 \pmod{1373652} \\ 3^{343413} &\equiv 1 \pmod{1373652} \end{aligned}$$

这也就是说， 1373653是基2和3的强伪素数。

(13)

(i)

注意到

$$\begin{aligned} n-1 &= (6m+1)(12m+1)(18m+1)-1 \\ &= 36m+396m^2+1296m^3 \end{aligned}$$

因为

$$\begin{aligned} 6m &\mid 36m+396m^2+1296m^3 \\ 12m &\mid 36m+396m^2+1296m^3 \\ 18m &\mid 36m+396m^2+1296m^3 \end{aligned}$$

所以根据Korselt定理， 这个数是Carmichael数。

(ii)

1

$$1729 = 7 \times 13 \times 19$$

是Carmichael数， 因为这是(i)中$m=1$的情况

2

$$294409 = 37 \times 73 \times 109$$

是Carmichael数， 因为这是(i)中$m=6$的情况

3

$$55164051 = 211 \times 421 \times 621$$

不是Carmichael数， 因为

$$210 \nmid 55164050$$

4

$$118901521 = 271 \times 541 \times 811$$

是Carmichael数， 因为这是(i)中$m = 45$的情况

5

这道题题目似乎有误， 应该为：

$$172947529 = 307 \times 613 \times 919$$

是Carmichael数， 因为

$$\begin{aligned} 306 &\mid 172947528 \\ 612 &\mid 172947528 \\ 918 &\mid 172947528 \end{aligned}$$

(14)

首先，

$$561 = 3 \times 11 \times 17$$

然后求得：

$$\begin{aligned} \left(\frac{2}{561}\right) &= \left(\frac{2}{3}\right)\left(\frac{2}{11}\right)\left(\frac{2}{17}\right) \\ &= -1 \times -1 \times 1 \\ &= 1 \end{aligned}$$

这说明， 561是基2的Euler伪素数。

(19)

首先

$$25326001 = 2251 \times 11251$$

这说明它是合数。

然后，

$$\begin{aligned} 25326000 &= 2^2 \times 1582875 \\ 2^{1582875} &\equiv -1 \pmod{25326001} \\ 3^{1582875} &\equiv -1 \pmod{25326001} \\ 5^{1582875} &\equiv 1 \pmod{25326001} \end{aligned}$$

这说明， 25326001是基2， 3， 5的强伪素数。