计算机安全 作业2

2018年12月9日 11:44

姓名：	芮志清
学号：	2018Z8020661080
班级：	人工智能学院2018级非全日制8班
邮箱：	ruizhiqing18@mails.ucas.ac.cn

8.4 利用费马定理计算$3^{201} \bmod 11$。

答：

由于3,11互素

根据费马定理，得

$3^{10} \equiv 1 \ (\mathrm{mod}\ 11)$

$3^{201} = 3^{10} * 3^{10} * 3^{10} * \cdots * 3^{10} * 1$

$3^{201} \bmod 11 = 1 * 1 * 1 * \cdots * 1 * 3 (\mathrm{mod}\ 11)$

$= 3 \ (\mathrm{mod}\ 11)$

8.6 利用费马定理，找一个位于0到28之间的数x, 使得x^{85} 模29与6同余。（不能穷举）

x=0时，$x^{85} \bmod 29 = 0 \neq 6$

当$x \in [1,28]$时, $GCD(x, 29) = 1$

$x^{28} \equiv 1 \ (\mathrm{mod}\ 29)$

$x^{85} = x^{28} * x^{28} * x^{28} * x$

$x^{85} \equiv x \ (\mathrm{mod}\ 29) \equiv 6 \ (\mathrm{mod}\ 29)$

$\therefore x = 6$

8.8 利用欧拉定理，找一个位于0到28之间的数x, 使得x^{85} 模35与6同余。（不能穷举）

由欧拉定理，$\varphi(35) = 24$

若x与35互素,则$x \neq 5, x \neq 7$，$x^{\varphi(35)} \equiv x^{24} \equiv 1 \ (\mathrm{mod}\ 35)$

$x^{85} = x^{24} * x^{24} * x^{24} * x^{13} \equiv 1 * 1 * 1 * x^{13} (\mathrm{mod}\ 35) \equiv 6 (\mathrm{mod}\ 35)$

两边平方： $x^{26} \equiv 36 (\mathrm{mod}\ 35) \equiv 1 (\mathrm{mod}\ 35)$

$\equiv x^{24} * x^{2} \ (\mathrm{mod} 35) \equiv x^{2} \ (\mathrm{mod} 35) \equiv 1 \ (\mathrm{mod}\ 35)$

$\therefore x = 6$