实验课 2

计算 $a^n \bmod p$，其中 a，n 和 p 均为正整数，均可用 32 位整型变量存储。

从屏幕中输入 a，n 和 p。

要求：循环次数不超过 32 次。不得采用递归等尚未介绍的课程内容。

提示：n 为偶数时，$a^n \equiv a^{n/2} a^{n/2} (\bmod p)$；$n$ 为非负整数时，$\lfloor n/2 \rfloor$（向下取整）也可通过位运算 n >> 1 实现。

另，若 n 的二进制表示为：$(b_{k-1}, \ldots, b_0)_2$，那么有：

$$
\begin{aligned}
a^n &= a^{(b_{k-1},\ldots,b_0)_2} \\
&= a^{b_{k-1}\cdot 2^{k-1}} \cdots a^{b_0 \cdot 2^0}
\end{aligned}
$$

注意，$b_j (0 \le j < k)$ 要么为 0，要么为 1，所以，上式的关键在于计算出：$a^{2^0}, a^{2^1}, \ldots, a^{2^{k-1}}$，而同时注意到：$a^{2^{k-1}} = a^{2^{k-2}} \cdot a^{2^{k-2}}$。

实验报告要求：

1. 撰写实验报告，报告需解释思路，并截图表示代码运行结果。
2. 完整代码作为附录放在实验报告的最后。
3. 在华为云上进行测试，注意，gcc 编译的参数和之前类似。请自己多琢磨琢磨。

关键事宜：华为云开机后用完后，记得关机！

如下：

控制台：


华为云
控制台
北京四
搜索
费用中心
资源
工单
企业
开发工具
备案
支持与服务
中文（简体）
云服务器控制台
总览
弹性云服务器
专属主机
裸金属服务器
云硬盘
专属分布式存储
镜像服务
弹性云服务器
最新动态
使用指南
诚邀您参加弹性云服务器使用体验调研，您宝贵的意见和建议是我们持续提升产品体验的源动力，感谢您的参与！
开机
关机
重置密码
更多
默认按照名称搜索
名称/ID
监控
可用区
状态
规格/镜像
IP地址
计费模式
标签
操作
ecs-16d0
00d8df8d-e053-4a62-ba68...
可用区2
关机
1vCPUs | 1GB | kc1.smal...
openEuler 20.03 64bit w...
124.70.0.227 (...
192.168.1.224 (...
按需计费
2021/04/02 10:3...
--
远程登录