第五运算、费马数与费马小定理（Fermat）2012-9-22

1. **理解：幂次方，我们称之为第五运算（加减乘除、乘方、开方）**

**趣题：给定三个2，不许用运算符号，写出尽可能大的数。**

（222, 222=484，（2^2）^2=16，真正最大的是222=4 194 304）

**三个3呢，**

（3^(3^3)=3^27=7625597484987, 最大是3^33=5559060566555523）

**三个四呢**

（4^44=309485009821345068724781056，4^（4^4）=4^256>4^44）

**一般的，何时, a>1的正整数，即 ,**

**显然当a ≥4时，上式成立。**

**补充幂次方运算的规则：**

**n个a连乘，数学上为了节省时间，简写成：an, 本质就是n个相同的a连乘结果。**

****

1. **形如 的数称为费马数，证明：当n≥2时，Fn的末位数字是7.**

证明：当n≥2时，2n是4的倍数，不妨设2n=4t，t为大于1的正整数,从而费马数为

，即费马数Fn的末位数字是7。()

注：费马数的头几个为：，它们都是素数，费马据此猜测，对所有的正整数n，Fn都是素数。不过这一猜测是错误的，欧拉 证明了F5就不是素数。

F5=232+1=429 496 729 7=641x670 041 7是合数。

**Pierre de Fermat：皮埃尔·德·费马**，法国律师和业余数学家。他在数学上的成就不比职业数学家差，对数论最有兴趣，亦对现代微积分的建立有所贡献。被誉为“**业余数学家之王**”。

1. **费马大定理：也称费马最后定理，方程在整数且下，没有整数解【没有正整数解】。这个定理原来只是猜想，经过350多年，才被英国数学家Andrew Wiles（怀尔斯）和他的学生Richard Taylor（泰勒）在1995年所证明，发表在1995年5月的《数学年刊》上。**
2. **费马小定理**

**若p为素数，（a，p）=1，则ap-1≡1(mod p),**

假如p是质数，且a,p互质，那么 a的(p-1)次方除以p的余数恒等于1**。**

**逆定理不成立（中国猜想错误，反例p=341=11x31，满足 2341≡2（mod341））。**

**推论：对任意正整数a，有ap≡a （mod p） ，因为a能被p整除时，结论显然成立。**

**另外的描述是 p|(ap-1-1), 或 p|(ap-a)。**

**注1：化为与±1同余，是我们经常要用的方法。**

**注2：证明还需要很多预备知识，在此略过。**

**注3：初等数论四大定理：中国剩余定理，欧拉定理，费马小定理和**

**威尔逊定理（（p-1）！≡-1 （mod p）等价于 p是素数）。**

1. **求出258000除以7的余数是多少?**

解: ∵（25,7）=1，7是素数，∴由费马小定理知 256≡1（mod 7），且25≡4（mod 7）

8000=6×1333+2， 258000=（256）1333×252≡42≡2（mod 7）

1. **假设p为任意一个大于5的质数，证明：p必整除N=111…1(假设这是十进制中由p-1个1构成的数)。**

证明：∵ p>5,且（p，10）=1，∴由费马小定理得 10p-1≡1(mod p), 又

9N=10p-1-1，故p|（9N），（p，9）=1，从而 p|N。

1. **求19932000除以17的余数。**

解：∵17是素数，17不能整除1993，（17,1993）=1，

∴由费马小定理得到 199316≡1（mod 17）

19932000=（199316）125≡1（mod 17），即19932000除以17的余数为1

1. **证明：5|（1241+2241+3241+4241），但 1240+2240+3240+4240不能被5整除。**

证明：5是素数，且1,2,3,4与5互素，由费马小定理知：

a4≡1（mod 5）,而 a241=（a4）60a≡a（mod 5），此处a为1，2，3，4

所以（1241+2241+3241+4241）≡（1+2+3+4）≡0（mod 5）

但是 1240+2240+3240+4240≡1+1+1+1≡4（mod 5）

故5不能整除1240+2240+3240+4240，但能整除1241+2241+3241+4241

1. **证明：2730|n13-n**

补充：

证明：2730=2×3×5×7×13，记f(n,k)= nk-n, 由费马小定理得知：k|f(n,k),k=2,3,5,7,13,即

n13≡n（mod 13），

n7≡n（mod 7），

n5≡n（mod 5），

n3≡n（mod 3），【3|(n-1)n(n+1), 意味着连续三个自然数的乘积是3的倍数】

n2≡n（mod 2），【2|n(n-1)，意味着两个连续自然数的乘积为偶数】

∵n13-n=n（n12-1）=n（n6-1）（n6+1），∴n7-n| n13-n，同理

f(n,13)=n(n3-1)(n3+1)(n6+1)

=n(n-1)(n+1)(n2+n+1)(n2-n+1)(n2+1)(n4-n2+1)

故 n5-n| n13-n，n3-n| n13-n，n2-n| n13-n，

∴a| n13-n，a=2,3,5,7,13，且2,3,5,7,13两两互素，因此原结论成立。

1. **素数的判断定理**

**判断正整数n是否为素数，只需判断小于√n的素数a（a可取2,3,5,7，…）是否整除n，如果都不能整除n，说明n是素数。**

**定理：设正整数n，对于所有的素数，都有 n mod p≠0，则n一定是素数。**

**以下就是100以内的素数列表（共25个，除了一位素数外，其它素数的末尾都是1,3,7,9）**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **2** | **3** |  | **5** |  | **7** |  |  |  |
| **11** |  | **13** |  |  |  | **17** |  | **19** |  |
|  |  | **23** |  |  |  |  |  | **29** |  |
| **31** |  |  |  |  |  | **37** |  |  |  |
| **41** |  | **43** |  |  |  | **47** |  |  |  |
|  |  | **53** |  |  |  |  |  | **59** |  |
| **61** |  |  |  |  |  | **67** |  |  |  |
| **71** |  | **73** |  |  |  |  |  | **79** |  |
|  |  | **83** |  |  |  |  |  | **89** |  |
|  |  |  |  |  |  | **97** |  |  |  |

**如果利用费马小定理：可以快速识别合数，只要求an-1 mod n，如果不是1，就一定不是素数。这个方法不能保证测试的n一定是素数，但是可以有效发现合数，可以在判断素数的过程中提供初步而快速的筛选，被很多实际程序所采纳。**

1. **求证：当p为素数且不等于2时，np-n必定可被2p整除。**

证明：由费马小定理，p|(np-n), ①

当n为偶数时，np-n=n(np-1-1)显然能被2整除；

当n为奇数时，n ≡1（mod 2），故 np-n≡1-1≡0（mod 2）, 故2| (np-n) ②

由①、②以及（2，p）=1，得到 2p| （np-n）

1. **求33除22012的余数。**

解：先找出与±1（mod 33）同余的数，∵25=32≡-1（mod 33），

∴210=（25）2≡（-1）2≡1（mod 33），

22012=22010×22 =（25）402×4≡（-1）402×4≡4 （mod 33）。

1. **求8除72n+1-1的余数。**

解：∵7≡-1（mod 8）∴72n+1≡（-1）2n+1≡-1（mod 8），故72n+1-1≡-1-1≡-2≡6（mod 8）。即余数为6.

1. **求15+25+35+…+995+1005除以4所得的余数。**

解：观察是连续自然数的5次方的和，分偶数和奇数讨论。

∵ 4|(2n)5， ∴(2n)5≡0（mod 4）；

∵(2n+1)2=4n(n+1)+1, ∴(2n+1)2≡1(mod 4), (2n+1)5≡2n+1(mod 4)

∴