Problem Set 9：数论初步

提交截止时间：4 月 8 日 10:00 前

Problem 1

设 a, b, c, d 均为正整数，下列命题是否为真？若为真，给出证明；否则，给出反例。
a. 若 a | c, b | c, 则 ab | c

```
⊥
a = 6
b = 10
c = 30
```

b. 若 a | c, b | d, 则 ab | cd

```
T
c = x * a (x ∈ Z)
d = y * b (y ∈ Z)
c * d = (a * b) * (x * y)
所以
ab | cd
```

c. 若 ab | c, 则 a | c

```
T
c = (ab) * x (x ∈ Z)
所以 c % z = b * x
```

d. 若 a | bc, 则 a | b 或 a | c

```
⊥
b = 2
c = 3
a = 6
```

Problem 2

证明：若p是大于3的素数，则p^2-1是24的倍数。

```
因为p是大于3的质数，p一定不是3的倍数，并且p是奇数
(p+1) * (p-1)是两个连续的偶数，必定是8的倍数
p不是3的倍数，p+1,p-1必定有一个是3的倍数
所以p^2-1是24的倍数

```

Problem 3

计算：
a. 23300 mod 11
因为
$=23300^{10} mod 11$
$=(233 mod 11)*(100 mod 11)$
$=2$

b. 23300 mod 31
$=((233 mod 31)*(100 mod 31)) mod 31$
$=(7*16) mod 31$
$=19$

$c. 3^{516} mod 7$
$=(3^6)^{86} mod 7$
$=1^{86} mod 7$
$=1$

Problem 4

试证明：对于任意的正整数n，都有$n^2|(n+1)^n-1$。

当n = 1时，原式成立
假设当$n=k$时，原式成立, $k^2|(k+1)^k-1$
当$n=k+1$, 原式等于$(k+1)*((k+1)^k-1)+(k+1)-1$
根据假设条件, 设$(k+1)^k=m*k^2$
原式等于
$k^2*((k+1)*m+1)$
因此命题成立

Problem 5

证明：如果a和b为正整数，则$(2^a-1)mod(2^b-1)=2^{amodb}-1$。
当b = 1 时, 原式成立
假设b = k时候，原式成立
当b = k + 1时，
$(2^a-1)mod(2^{k+1}-1)$
$=(2^a-1)mod(2^k*2-1)$
$=((2^a-1)mod(2^k-1)*(2^kmod(2^k-1)))$
所以
$(2^a-1)mod(2^{k+1}-1)$
$=(2^{amodk}-1)*(2^k-1)+(2^{amodk}-1)$
$=(2^{amodk+k}-(2^k-1)+2^{amodk})-1$
$=2^{amod(k+1)}-1$

Problem 6

证明：如果2^n-1是质数，则n也为质数。
假设$\exists n\in Z+$使得2^n-1是一个质数，但n不是一个质数，
即$n=a*b$
但$2^n-1=2^{a*b}-1=(2^a-1)*(2^{a*(b-2)+...+2^a+1})$
因为n是2^n-1的质因数所以2^n-1不能分解为两个质因数的乘积
得出矛盾，所以假设错误，该命题得证

Problem 7

证明:
a. 设 d ≥ 1, d | m, 则 a ≡ b(mod m) ⇒ a ≡ b(mod d).

```
不妨假设 x = a % m = b % m
根据题意
a % d = x % d = b % d
得证
```

b. 设 d ≥ 1, 则 a ≡ b(mod m) ⇔ da ≡ db(mod dm).

```
设 b = p * m + k, a = q * m + k
两边同时乘以d
可得db = dp * dm + dk, da = dq * dm + dk
所以 da ≡ db (mod dm)
只需将构造过程逆向即可以从右边推出左边
```

c. 设 c 与 m 互质, 则 a ≡ b(mod m) ⇔ ca ≡ cb(mod m).

```
不妨假设b = p * m + k, a = q * m + k
根据上题目构造方式可得
ca mod m = ck mod m = cb mod m
所以命题成立
只需将构造过程逆向即可以从右边推出左边
```

Problem 8

借助于费马小定理证明如果n是一个正整数，则42能整除n^7-n。
mod2
如果n为偶数，$n^7\equiv n\equiv 0$
如果n为奇数，$n^7\equiv n\equiv 1$

mod3
如果n是3的倍数，则n^7和n都是3的倍数，$n^7\equiv n\equiv 0$
否则，$n^2\equiv 1,$所以$n^7\equiv 1*1*1*1*n$

mod7
如果 n 是7的倍数，则n ^ {7}和n都是7的倍数，n ^ {7} ≡ n ≡ 0
否则, $n^6\equiv 1, n^7\equiv n^6*n\equiv n$

所以n^7-n对于$(2*3*7)$模同余

Problem 9

试证明：若$p\geq 7$为质数，则$240|(p^4-1)$。
mod2
因为p是质数，所以$p^4\equiv 1$

mod3
据费马小定理，$p^2\equiv 1,$所以$p^4\equiv 1$

mod5
据费马小定理，$p^4\equiv 1$
所以p^4-1对于(2^4*3*7)模同余

Problem 10

证明*:* 若m和n互质，则$m^{\phi(n)} + n^{\phi(m)} \equiv 1 (mod mn)$.