1、请确定以下对应的乘法群中所有元素的阶，并确定哪些元素是本原元：

（1）$\mathbb{Z}_5^*$

（2）$\mathbb{Z}_7^*$

（3）$\mathbb{Z}_{13}^*$

2、对于群$\mathbb{Z}_{53}^*$，元素的阶的取值有哪些？对每个阶而言，存在多少个元素？

3、对于群$\mathbb{Z}_{53}^*$，有多少个子群？找出$\mathbb{Z}_{53}^*$的所有子群和每个子群的本原元。

解：(1) $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

mod 5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1: $k=1$

2: 2^1 2^2 2^3 2^4

√ 2 4 3 1

$k=4$

3^1 3^2 3^3 3^4 ×　　4^1 4^2　$k=2$

3 4 2 1　$k=4$　　4 1

故 $ord(1)=1$, $ord(2)=4$, $ord(3)=4$, $ord(4)=1$

其中2,3为本原元

(2) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ $|G|=6=2\times3$ 故生成元做为 $\varphi(6)=(2-1)(3-1)=2$

分别 1: $ord(1)=1$

2: 2^1 2^2 2^3　$ord(2)=3$

2 4 1

3: 3^1 3^2 3^3 3^4 3^5 3^6　$ord(3)=6$

3 2 6 4 2 1

4. 4^1 4^2 4^3　$ord(4)=3$

4 2 1

5. 5^1 5^2 5^3 5^4 5^5 5^6

5 4 6 2 3 1　$ord(5)=6$

6. 6^1 6^2 $ord(6)=2$

6 1

如上，其中 3 和 5 为本原元

(3) $\mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$.

$|G|=12$，含有的因数有 1, 2, 3, 4, 6, 12 即元素的阶的取值范围.

1: $ord(1)=1$

2: $2^1 \bmod 13 = 2$, $2^2 \bmod 13 = 4$, $2^3 \bmod 13 = 8$, $2^4 \bmod 13 = 3$

$2^5 \bmod 13 = 6$, $2^6 \bmod 13 = 12$, $2^{12} \bmod 13 = 1$ $ord(2)=13$

…… 由欧拉定理 $gcd(a,13)=1$

$a^{\varphi(13)} \equiv 1 \pmod{13}$ 又 $\varphi(13)=12$

即 $a^{12} \equiv 1 \pmod{13}$ 故剩余元素的阶均为12

且本原元为除了 1 的其它元素

2. ∵ $ord|a|$ 可整除 $|G|$

$|G|=12$，其因数有 1, 2, 4, 3, 6, 12

故为元素所的取值

又在循环群中，阶为 n 的元有 $\varphi(n)$ 个

当 $n=1$ 时，有 1 个阶为 1 的元素

同理，有 $\varphi(2)=1$，故有 1 个阶为 2 元素

$\varphi(4)=2$，有 2 个阶为 4 元素

$\varphi(13) = 12$, 有12个阶为13元素

$\varphi(26) = 12$, 有12个阶为26元素

$\varphi(52) = 24$, 有24个阶为52元素

3. 由于每个阶对应一个子群, 而52的因子有

1, 2, 4, 13, 26, 52 共6个, 故有6个循环子群

又由拉格朗日定理的推论.

阶为k的循环子群H, H由 $a^{n/k}$ 生成.

阶为1时, 子群为 $\{C(1), 0\}$

k=2时, 子群为 $\{(52), 0\}$

k=4时, 子群为 $\{(23, 30), 0\}$

k=13时, 子群为 $\{(10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49), 0\}$

⋮

k=52时, 子群为: $\{(2, 5, 8, 10, 14, 18, 19, 20, 21, 22, 24, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 5)\}$

每个循环子群中的每个元素也均为生成元