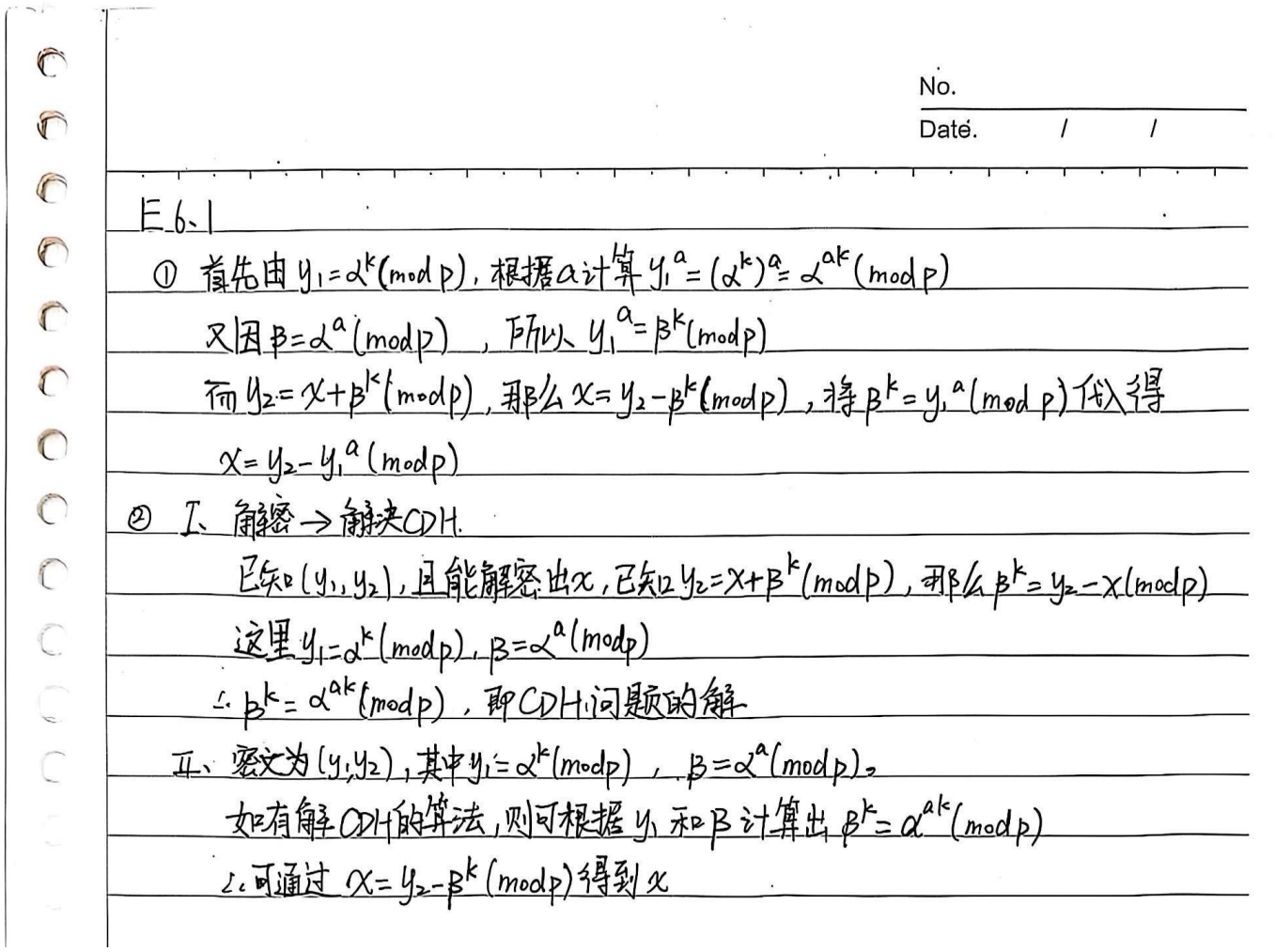

习题 6.20

源代码：

```
def modinv(a, p):
    return pow(a, -1, p)


def L1_table_gen(alpha, p):
    table = {}
    val = 1
    for i in range(p):
        table[val] = i
        val = (val * alpha) % p
    return table


def L2_oracle(beta):
    if beta in [25219, 841]:
        return 1
    elif beta in [163, 532, 625, 656]:
        return 0
    else:
        return -1  # undefined
```

```python
def log_discrete(p, alpha, beta):
    L1 = L1_table_gen(alpha, p)
    x = []
    b = beta

    x0 = L1[b]
    x.append(x0)
    b = (b * modinv(pow(alpha, x0, p), p)) % p

    i = 1
    while b != 1:
        xi = L2_oracle(b)
        x.append(xi)
        gamma = pow(b, (p + 1) // 4, p)
        if L1[gamma] == xi:
            b = gamma
        else:
            b = (p - gamma) % p
        b = (b * modinv(pow(alpha, xi, p), p)) % p
        i += 1

    return sum(xi * (1 << i) for i, xi in enumerate(reversed(x)))

# 使用
p = 1103
alpha = 5
beta = 896
result = log_discrete(p, alpha, beta)
print("log_5 896 =", result)
```

结果：

```
log_5 896 = 147
```