Test for Number Theory

Something you should know...

$gcd(a,b)$ is the greatest common divisor of a and b.

$lcm(a,b)$ is the least common multiple of a and b.

$a \equiv b \pmod{p}$ indicates that $a \bmod p = b \bmod p$.

$\sum_{i=1}^{n} a_i$ is equal to $a_1 + a_2 + \cdots + a_n$.

$\prod_{i=1}^{n} a_i$ is equal to $a_1 a_2 \cdots a_n$.

$\varepsilon(n)$ is the unit function.

$1(n)$ is the constant function.

$Id_k(n)$ is the identity function.

$\sigma_k(n)$ is the divisor function.

$\varphi(n)$ is the Euler totient function.

$\mu(n)$ is the Mobius function.

We assume that the multiplicative inverse with respect to the modulus p is always between 1 and $p-1$.

I. Multiple choice

> There is exactly one correct answer.

1. (3pts) Which of the following integers is a divisor of 247?

   A. 7 B. 11 C. 13 D. 17

2. (3pts) Which of the following integers is a prime?

   A. 179 B. 187 C. 133 D. 154

3. (3pts) Which of the following integers has the maximum number of factors?

   A. 24 B. 30 C. 50 D. 80

4. (3pts) Which of the following integers is congruent to 100 with respect to the modulus 7?

   A. 39 B. 57 C. 65 D. 82

5. (3pts) Which of the following functions is the Dirichlet inverse of μ?

   A. 1 B. Id C. σ D. φ

II. Fill in the blanks

> No need to write the steps.

6. (4pts) Represent 58212 using the product of primes. $58212 =$( ).
7. (4pts) The least common multiple of 24, 33 and 56 is ( ).
8. (4pts) Find the solution of $60x + 96y = 12$ while $|x| + |y|$ is minimum. $x =$( ), $y =$( ).
9. (4pts) Find the multiplicative inverse of 8 with respect to the modulus 17. $8^{-1} \equiv$( ) $(\mathrm{mod}\ 17)$.
10. (4pts) Find the value of $\sum_{d|30030} \varphi(d)$. $\sum_{d|30030} \varphi(d) =$( ).

III. Calculation

> Need to write the steps in detail.

11. (7pts) Find the multiplicative inverse of 313 with respect to the modulus 1237 using extended Euclidean algorithm.
12. (7pts) Find the multiplicative inverse of 2, 3, 4, 5 and 6 with respect to the modulus 314159 using recursive method. Hint: $(p - i)x \equiv p - ix \pmod{p}$.
13. (7pts) Find the minimum positive solution of the following equations using Chinese remainder theorem.

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

14. (8pts) Find the value of $3^{290} \bmod 360$.
15. (8pts) Find the value of $\sum_{i=1}^{40} \left\lfloor \frac{40}{i} \right\rfloor$.

IV. Proof

> Need to write the steps in detail.

16. (7pts) Prove that $gcd(a, b) \cdot lcm(a, b) = ab$.
17. (7pts) Given the program of Euler sieve. Prove that the time complexity is $O(N)$.

```
bool vis[N];
int cnt, prime[N], mu[N];

for (int i = 2; i < N; ++i) {
    if (!vis[i]) {
        prime[cnt++] = i;
        ___(18.1)___
    }
    for (int j = 0; j < cnt && i * prime[j] < N; ++j) {
        vis[i * prime[j]] = 1;
        if (i % prime[j] == 0) {
            ___(18.2)___
            break;
        } else {
            ___(18.3)___
        }
```

```
    }
}
```

18. (6pts) Complete the program to calculate μ (the value should be stored in `mu[]`).
19. (8pts) Prove that $Id * d = 1 * \sigma$, where $Id = Id_1$, $d = \sigma_0$, $\sigma = \sigma_1$.
20. (extra 5pts) Assume that $n = pq$, where p and q are two different primes. Prove that $p^{pq-p-q+2} \equiv p \pmod{n}$. Note that p and n are not coprime, but p and q are coprime.