Практическое задание 1

Задание 1 Модульная арифметика. (3 балла, $\frac{1}{12}$ за каждое задание).

1. $x \equiv 12 mod 5$
   $x \equiv 2 mod 5$
   $x = 5k + 2$
2. $x \equiv 12 mod 6$
   $x \equiv 0 mod 6$
   $x = 6k$
3. $x \equiv -1 mod 13$
   $x \equiv 12 mod 13$
   $x = 13k + 12$
4. $x \equiv 119 mod 5$
   $x \equiv 4 mod 5$
   $x = 5k + 4$
5. $x \equiv -144 mod 7$
   $x \equiv -4 mod 7$
   $x \equiv 3 mod 7$
   $x = 7k + 3$
6. $x \equiv -656 mod 13$
   $x \equiv -6 mod 13$
   $x \equiv 7 mod 13$
   $x = 13k + 7$
7. $x \equiv 1000 mod 11$
   $x \equiv 10 mod 11$
   $x = 11k + 10$
8. $x \equiv 1234 mod 1$
   $x \equiv 0 mod 1$
   x - любое целое число
9. $x \equiv 3n mod 3$
   x=0
10. $x \equiv (2n + 1) mod 2$
    $x \equiv (2n) mod 2 + 1 mod 2$
    x=1
11. $x \equiv 15n^4 + 9n^2 + 2 mod 3$
    x=2 - по аналогии с 10

12. $x \equiv 9 + 4 (mod 12)$
    $x \equiv 13 mod 12$
    $x \equiv 1 mod 12$
    $x = 12k + 1$
13. $x \equiv 3 + 9 (mod 12)$
    $x = 12k$
14. $x \equiv 7 + 8 (mod 21)$
    $x \equiv 15 mod 21$
    $x = 21k + 15$
15. $x \equiv 7 - 8 (mod 21)$
    $x \equiv -1 mod 21$
    $x \equiv 20 mod 21$
    $x = 21k + 20$
16. $x \equiv 3 - 10 (mod 15)$
    $x \equiv -7 mod 15$
    $x \equiv 8 mod 15$
    $x = 15k + 8$
17. $x \equiv 10 - 3 (mod 15)$
    $x \equiv 7 mod 15$
    $x = 15k + 7$
18. $x \equiv 7 \cdot 8 (mod 15)$
    $x \equiv 56 mod 15$
    $x \equiv 11 mod 15$
    $x = 15k + 11$
19. $x \equiv 6 \cdot 10 (mod 15)$
    $x \equiv 60 mod 15$
    $x \equiv 0 mod 15$
    $x = 15k$
20. $x \equiv 14 \cdot 14 (mod 15)$
    $x \equiv 196 mod 15$
    $x \equiv 1 mod 15$
    $x = 15k + 1$
21. $x \equiv 3^2 (mod 15)$
    $x \equiv 9 mod 15$
    $x = 15k + 9$
22. $x \equiv 3^4 (mod 15)$
    $x \equiv 6 mod 15$
    $x = 15k + 6$
23. $x \equiv 3^6 (mod 7)$
    $x \equiv 729 mod 7$
    $x \equiv 1 mod 7$
    $x = 7k + 1$

24. $gcd(56, 76) = 4$
    НОД(76,56)
    76=56*1+20
    56=20*2+16
    20=16*1+4
    16=4*4+0
25. $\varphi(10)$
    10=2*5
    $\varphi(10) = \varphi(2) * \varphi(5) = (2-1) * (5-1) = 4$
26. $\varphi(37) = (37-1) = 36$
27. $\varphi(38) = (2-1) * (19-1) = 18$

Задание 2 Фундаментальная теорема номера ИСУ. (1 балл).

Дано

Найдите каноническую форму своего номера ИСУ.
Подсказка: Фундаментальная теорема арифметики.
Номер ИСУ - 370864

Решение

Каноническую форму находим с помощью скрипта:

```
a = 370864
divs = []
b = 2
while a > 1:
    while a%b != 0:
        b+=1
    divs.append(b)
    a /= b
    b = 2
print(divs)
```

Ответ: $370864 = 2^4 * 13 * 1783$

Задание 3 Наименьшее общее кратное (1 балл).

Дано

Найдите НОК от вашего номера ИСУ и следующего по спику +
4 по модую {количество человек в группе + 1} :D
Номер ИСУ - 370864

Номер ИСУ следующего - 270222
Кол-во человек в группе - 25

Решение

НОК(370864, (270222+4)%(25+1))
НОК(370864, 8)
Найдем НОК с помощью скрипта:

```
a = 370864
b = 8
l = max(a,b)
while True:
   if l%a==0 and l%b==0:
       print(l)
       break
   l += 1
```

Ответ: 370864

Задание 4 Алгоритм быстрого возведения в степень (1 балл).

Дано

Посчитайте:
$17^{189} mod(200)$

Решение

$17^{189} mod(200)$
189 = 128+32+16+8+4+1 = 10111101
$17^1 = 17 mod(200)$
$17^2 = 89(200)$
$17^4 = 121 mod(200)$
$17^8 = 41(200)$
$17^{16} = 81(200)$
$17^{32} = 161(200)$
$17^{64} = 121(200)$
$17^{128} = 41(200)$
$(41 * 161 * 81 * 41 * 121 * 17) mod(200) = 45093391497 mod(200) = 97$
Ответ: 97

Задание 5 Очумелые ручки (1 балл).

Дано

$(1! + 2! + 3! + \ldots + 2022!) mod(8)$
Получите в 4 раза больше если решите ручками в тетради

Решение

$1! mod(8) = 1$
$2! mod(8) = 1 * 2 = 2 mod(8) = 2$
$3! mod(8) = 1 * 2 * 3 mod(8) = 6 mod(8) = 6$
$4! mod(8) = 1 * 2 * 3 * 4 mod(8) = 24 mod(8) = 0$
$5! mod(8) = 5 * 4 mod(8) = 5 * 0 = 0$
$6! mod(8) = 6 * 5 * 4 mod(8) = 6 * 5 * 0 = 0$
...
$(1! + 2! + 3! + \ldots + 2022!) mod(8) = (1 + 2 + 6) mod(8) = 1$
Ответ: 1

Задание 6 Взлом RSA (5 баллов).

Необходимо прочитать и понять, как работает алгоритм шифрования RSA.

RSA - ассиметричное шифрование.

Генерация пары ключей (открытый, закрытый).

1. Взять 2 случайных простых числа (чем больше, тем безопаснее) - p и q
2. Вычислить модуль n=p*q
3. Выбрать простое число e, так чтобы оно было взаимно простым со значением функции Эйлера от n. e - открытая экспонента
4. Вычислить число d по уравнению d*e=1(mod(φ(n)). d - секретная экспонента
5. Открытый ключ - (e, n)
6. Закрытый ключ - (d, n)

Шифрование

Для шифрования необходимо знать:

- e - открытая экспонента
- n - модуль
- (e, n) - открытый ключ
- m - открытый текст
  $c = m^e mod(n)$, где c - секретное сообщение

Расшифрование

Для расшифрования необходимо знать:

- d - секретная экспонента
- n - модуль
- (d, n) - закрытый ключ
- c - секретное сообщение
  $m = c^d mod(n)$, где m - расшифрованное сообщение

Далее Боб шифрует некоторое сообщение m и отправляет его Алисе. Помогите Еве узнать, какое сообщение было отправлено.

Дано

Открытый ключ Алисы(e,N):

- e = 17
- N = 29329
  Секретное сообщение Боба c:
- c = 16469

Решение

Расшифруем сообщение следующим образом:

1. Найдем p и q с помощью следующего скрипта:

```
n=29329
row = []
d = 2
while d * d <= n:
    if n % d == 0:
        row.append(d)
        n //= d
    else:
        d += 1
if n > 1:
    row.append(n)
print(row)
```

2. Расшифруем сообщение с помощью этого скрипта:

```
import gmpy2
c = 16469
n = 29329
e = 17
p = 139
q = 211
```

```
d = gmpy2.invert(e, (p-1)*(q-1))
m = pow(c,d,n)
print(m)
```

m - расшифрованное сообщение

Ответ: 14702