

2010 年度 「離散数学」 中間試験

1 (15 点) 30353 と 27007 の最大公約数 $g = \gcd(30353, 27007)$ を求めよ.

2 (20 点) 方程式 $21x \equiv 9 \pmod{51}$ の解で, 互いに合同でないものをすべて求めよ.

3 (15 点) フェルマーの小定理を使って方程式 $x^{244} \equiv 8 \pmod{23}$ を満たす x を mod 23 ですべて求めよ.

4 (15 点) 整数 m は, それが合成数であるにも拘らず, $\gcd(a, m) = 1$ なるすべての a について $a^{m-1} \equiv 1 \pmod{m}$ が成り立つとき, カーマイケル数と呼ばれる. $m = 1729 = 7 \times 13 \times 19$ がカーマイケル数であることを示せ.

Hint: まず, $\gcd(a, m) = 1$ ならば $a^{m-1} \equiv 1 \pmod{7}$, $a^{m-1} \equiv 1 \pmod{13}$, $a^{m-1} \equiv 1 \pmod{19}$ となる事を示せ.

学籍番号	氏名	
------	----	--

5 (25 点) 以下のメッセージを解読せよ. これは $m = 71 \times 89 = 6319$ を法とし, 指数を $k = 1021$ として送られてきたものである. ただし, 以下の値を利用してよい. \equiv は $\equiv (\text{mod } 6319)$ の略記である.

$$3886$$

$$3886^2 \equiv 4950, \quad 3886^4 \equiv 2592, \quad 3886^8 \equiv 1367, \quad 3886^{16} \equiv 4584, \quad 3886^{32} \equiv 2381, \quad 3886^{64} \equiv 1018,$$

$$3886^{128} \equiv 8, \quad 3886^{256} \equiv 64, \quad 3886^{512} \equiv 4096, \quad 3886^{1024} \equiv 271, \quad 3886^{2048} \equiv 3932, \quad 3886^{4096} \equiv 4350.$$

また, 変換は下記の表でなされたものとする.

00	01	02	03	04	05	06	07	08	09	10	11
い	ろ	は	に	ほ	へ	と	ち	り	ぬ	る	を

12	13	14	15	16	17	18	19	20	21	22
わ	か	よ	た	れ	そ	つ	ね	な	ら	む

23	24	25	26	27	28	29	30	31	32	33	34
う	る	の	お	く	や	ま	け	ふ	こ	へ	て

35	36	37	38	39	40	41	42	43	44	45	46	47
あ	さ	き	ゆ	め	み	し	ゑ	ひ	も	せ	す	ん

6 (10 点) $3^m \times 5^n$ の形の完全数は存在しないことを証明せよ. (Hint : $\frac{\sigma(3^m \times 5^n)}{3^m \times 5^n} < 2$ を示せ.)