2010.7.30

2010 年 度 「離 散 数 学」期 末 試 験

1 (15 点) 14317 と 24617 の最大公約数 $g = \gcd(14317, 24617)$ を求めよ.

2 (20 点) 方程式　$33x \equiv 9 \pmod{51}$　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　$x^{1352} \equiv 5 \pmod{31}$　を満たす x を mod 31 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 $a^{m-1} \equiv 1 \bmod m$ が成り立つとき, カーマイケル数と呼ばれる. $\boxed{m = 2465 = 5{\times}17{\times}29}$ がカーマイケル数であることを示せ.
Hint: まづ, $\gcd(a, m) = 1$ ならば $a^{m-1} \equiv 1 \pmod 5$, $a^{m-1} \equiv 1 \pmod{17}$, $a^{m-1} \equiv 1 \pmod{29}$ 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 $\equiv \pmod{6319}$ の略記である.

116

$116^2 \equiv 818$, $116^4 \equiv 5629$, $116^8 \equiv 2175$, $116^{16} \equiv 4013$, $116^{32} \equiv 3357$, $116^{64} \equiv 2672$,
$116^{128} \equiv 5433$, $116^{256} \equiv 1440$, $116^{512} \equiv 968$, $116^{1024} \equiv 1812$, $116^{2048} \equiv 3783$, $116^{4096} \equiv 4873$.

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	ゐ	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) $5^m \times 7^n$ の形の完全数は存在しないことを証明せよ. $\left(\text{Hint}: \dfrac{\sigma(5^m \times 7^n)}{5^m \times 7^n} < 2 \text{ を示せ.}\right)$

ここより下には記入しないで下さい