高校生のための現代数学講座　　東京大学
「数論と暗号」　　玉原国際セミナーハウス
講義 (3)　大島　利雄　　2005 年 9 月 10 日

「素因数分解にかかる時間」

2^n, 3^n, $n!$ $(n = 0, 1, 2, \ldots)$ の表

```
       1         2         4         8        16        32        64       128       256       512
    1024      2048      4096      8192     16384     32768     65536    131072    262144    524288
 1048576   2097152   4194304   8388608  16777216  33554432  67108864 134217728 28435456 536870912

       1         3         9         8        27        81       243       729      2187      6561
   19683     59049    177147    531441   1594323   4782969  14348907  43046721 129140163 387420489

 1   1   2   6   24   120   720   5040   40320   362880   10!=3628800   39916800   479001600   6227020800
```

2 進法への変換
ある自然数 n が与えられたとき，数が 0 になるまで，以下の手順で 0 または 1 を右から左に並べて書いていく。
・その数が偶数なら 2 で割る。0 を一つ書く。
・その数が奇数なら 1 を引き 2 で割る。1 を一つ書く。
書かれた数字の並びはもとの数の 2 進数表示となる。

$$\begin{aligned}
(13-1)\div 2 &= 6 & & 1_2\\
(6-0)\div 2 &= 3 & & 01_2\\
(3-1)\div 2 &= 1 & & 101_2\\
(1-1)\div 2 &= 0 & & 1101_2 = 1000_2 + 100_2 + 1 = 2^3 + 2^2 + 1 = 8 + 4 + 1 = 13
\end{aligned}$$

問. 11, 33, 66 を 2 進法で表せ.

問. 10 進法で k 桁の数が，2 進法で m 桁になったとすると，$3m \le 10k + 2$.
理由.　$2^4 = 16 > 10^1$, $2^7 = 128 > 10^2$, $2^{10} = 1024 > 10^3$
$\Rightarrow$ $2^{10a} \ge 10^{3a}$, $2^{10a+4} \ge 10^{3a+1}$, $2^{10a+7} \ge 10^{3a+2}$
10 進法で $3a$ 桁の数は 10^{3a} より小さいので，2^{10a} より小さく，2 進法で $10a$ 桁以下。同様に 10 進法で $3a + 1$ 桁の数は 2 進法で $10a + 4$ 桁以下、10 進法で $3a + 2$ 桁の数は，2 進法で $10a + 7$ 桁以下。いずれも $3m \le 10k + 2$。

問. Euclid の互除法で除算が $2m$ 回かかる小さい方の数は 2^m 以上．よって，小さい方の数が k 桁の場合に Euclid の互除法の割り算は，$\frac{20k+4}{3}$ 以下の回数で終了.
理由. 最大公約数を求める互除法の各除算では，大きい自然数をより小さい自然数で割って余りを求める。大きい方の数は余りの 2 倍以上であり，大きい方の数は 1 回前の小さい方の数で 2 回前の余り。よって小さい方の数は，2 回前は 2 倍以上。

大きな数を扱っても速く計算できるアルゴリズム
・2 つの数の最大公約数を求める：Euclid の互除法（桁数の 5 倍未満の除算回数)
・ある数で割った余りのみに注目した四則演算やベキ乗計算（ mod 計算）

問.　$2^4 =$ ___,　$2^8 \equiv$ ___ mod 133,　$2^{16} \equiv$ ___ mod 133,　$2^{32} \equiv$ ___ mod 133,
$2^{33} \equiv$ ___ mod 133,　$2^{66} \equiv$ ___ mod 133,　$2^{132} \equiv$ ___ mod 133.

素数判定法（自然数 n が素数かどうか判定する）
直接法：$\sqrt{n}$ 以下の自然数（素数）で割り切れるかどうかを確かめる.

Wilson の定理: n が素数 $\Leftrightarrow (n-2)! \equiv 1 \mod n$
問. $n = 3, 4, 5, 13, 15, 17$ のときに Wilson の定理を確かめよ（$13! \equiv$ ___ mod 17）.

フェルマー法：素数 p に対して成り立つフェルマーの小定理を使う.

$$m^{p-1} \equiv 1 \mod p \quad (m = 1, \ldots, p-1)$$

問. $n = 13, 15, 17, 133$ のときに底 m を 2 とおいて，フェルマー法を確かめよ.

Rabin-Miller 法：p が素数の時，以下が成り立つことを使う.

$$m^2 \equiv 1 \mod p \ \Rightarrow\ m \equiv \pm 1 \mod p$$

$n - 1 = 2^k q$（q:奇数）とおいたとき，以下が正しければ n は素数でない.

$$m^{2^j q} \not\equiv \pm 1 \mod n \quad (j = 0, \ldots, k-1)$$

問. $n = 17, 133$ のときに底 m を 2 とおいて，Rabin-Miller 法を確かめよ.

強疑素数：$2, 3, 5, 7$ を底とする 2.5×10^{10} 以下の強擬素数は 3215031751 のみ.

カーマイケル数：561, 1105, 1729, 2465, 2821, 6601, 8911,...

フェルマー数（$F_n = 2^{2^n} + 1$）

・$2^m + 1$ が素数ならば，$m = 2^n$ である（$\Leftarrow$ フェルマーの小定理）

・正 p 角形（p：素数）が作図可能 $\Leftrightarrow$ p はフェルマー素数.

$F_0 = 2^1 + 1 = 3,\ F_1 = 2^2 + 1 = 5,\ F_2 = 2^4 + 1 = 17,\ F_3 = 2^8 + 1 = 257,\ F_4 = 2^{16} + 1 = 65537$

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297641 = 641 \times 6700417$ (Euler)

$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 274177 \times 67280421310721$ (Landry:1880)

$F_7 = 2^{2^7} + 1 = 2^{128} + 1 = 59649589127497217 \times 5704689200685129054721$ (Morrison-Brillhart:1970)

・F_4 より大きなフェルマー素数は見つかっていない.

メルセンヌ数（$M_p = 2^p - 1$，p:素数）

・2 進法では $111\cdots111$ と 1 を $p-1$ 個並べた数.

・$2^m - 1$ が素数 $\Rightarrow$ m は素数.

・42(?) 番目のメルセンヌ素数：$M_{25964951} = 2^{25964951} - 1$ (7816230 桁)

$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8191,\ M_{17} = 131071,\ M_{19} = 524287$

$M_{23} = 8388607 = 47 \times 178481,\ M_{29} = 536870911 = 47 \times 11424913,\ M_{31} = 2147483647, \ldots$

M_pが素数：$p = 2, 3, \ldots, 31, 61, 89, 107, 127, 521, 607, \ldots, 3021377$(1998 年), 6972593(38 番目, 1999 年),
13466917(2001 年), 20996011(2003 年), 24036583(2004 年), 25964951(2005 年)

多項式時間　大きな数 n を扱う問題において，n の桁数を k とすると，その問題を解くために掛かるステップ数が $a \cdot k^b$ 回以下となるような n によらない a と b が取れるとき，多項式時間で解ける問題という.

・Euclid の互除法では，$a = 5, b = 1$ とできるので，多項式時間で解ける.

・素数判定に関しても多項式時間で解けるアルゴリズムが最近発見された（$b = 7.5$ 程度）.

・素因数分解については，多項式時間で解けるアルゴリズムは知られていない.

素因数分解（自然数 n の素因数 p を見つける）

・直接法：$\sqrt{n}$ 以下の自然数（素数）で割りきれるか調べる.

・ρ 法：$a_0 = 2,\ a_{k+1} \equiv a_k^2 + 1 \mod n$ と順に定め $a_{2k} \equiv a_k \mod p$ を捜す.

・$p-1$ 法：フェルマーの小定理を使う．GCD$(a^m - 1, n)$ を調べる.

・$p+1$ 法：$y_0 = 2,\ y_1 = 1,\ y_{k+1} = a \cdot y_k + b \cdot y_{k-1}$ で定まる Lucas 列の性質を使う.

・連分数法 (CFM)：$a^2 - nb^2 = r$ の r が平方数となる a, b を捜す.

・複数多項式 2 次ふるい法 (MPQS)：$a^2 \equiv r \mod n$ の r が平方数となるよう調整.

・数体ふるい法 (NFS)

・楕円曲線法 (ECM)：楕円曲線 $y^2 = x^3 + ax + b$ 上　$\mod p$ で考えた整数点の演算を使う.

$(x_1, y_1), (x_2, y_2)$ に対し $x_1 \neq x_2$ ならば $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$，$\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$ とおいて
$x_3 = \lambda^2 - x_1 - x_2$，$y_3 = -\lambda x_3 - \nu$ と定める.

素数の分布　k 桁の素数は，k が大きいときは大体 $2.3k$ 個に一つ程度存在.

参考

http://www.rkmath.rikkyo.ac.jp/~kida/ubasic.htm　(UBASIC)

http://faculty.ms.u-tokyo.ac.jp/users/tambara/lectures_for_highschool.htm