465_素数表など

2021年8月9日



❶　前回（464_）の2番目の記事で暗黒通信団の円周率100万桁表について書きました。その後あちこちHP内を見ていてAmazonに登録されている出版物なども目にしました。（先頭画像）

❷　ＰＤＦライブラリでは「素因数分解表500000個」などをダウンロードしました。yamaMath「55_素数表の作成」でもEXCELで100万までの素数一覧表を作ったことなどが思い出されましたので再掲することに。yamaMath 右上の検索窓で「55_素数表の作成」（「」は不要）をコピー・貼り付けで検索すれば一瞬で表示されることと思います。

s-800_yamaMath_検索窓.JPG



55_素数表の作成

プログラムを含むxlsmファイルはwebに載らないのでやむなくZIPに冷凍してありますが，悪意ある内容などは含んでいませんのでダウンロード後に解凍し，セキュリティの警告をコンテンツの有効化ボタンで通り抜けてから実行してみてください。

1000000(100万)を入力して実行ボタンを押すと，素数を探しながら1000単位で表にして行きます。100万まで作表したあとで，2000毎にページ区切りを入れていきますのでpdfにでも印刷すれば500ページの素数表ができるというわけです。

実行にどの程度時間がかかったのかは忘れていましたので，再掲にあたり再度実行してみますと終了のメッセージボタンが出るまでに

dell・・・ 3分36秒
fmv ・・・ 13分36秒　　というところです。

下に8p抜粋版をリンクしてありますから，クリックすると雰囲気を感じていただけるものと思います。「55_素数表の作成」ではマクロの説明pdfなども同梱しています。

100万までの素数表_500pのうち8p抜粋.pdf

❸　「462_BASICとセンター試験 数学Ⅱ B」では素因数分解のプログラムを扱いましたが，これに関連して授業でよく使う4桁数字をいくつか。

1001=7*11*13 ある先生の車のナンバー。

5040=2^4*3^2*5*7 学園バスや理事長の車のナンバー。
=10*9*8*7 =順列 10Ｐ4　とも。
（授業では２２２２３３５７を板書して組み合わせていきます。）
=組み替えると 7!=7*6*5*4*3*2*1 とも

（「セブン・ドッキリ・甲子園」はことあるたびに言うので
生徒も覚えてくれます。）

5963=67*89=1234・5963・6789　　ある先生の車のナンバー
=いちにいさんしーご苦労さん・ろくしちはちクッキリ東芝さん
(昔のＴＶ-ＣＭ・桂文枝
197X 東芝 ブラックストライプ
– YouTube [360p].mp4　を見せることも)

☆　「♪この木なんの木」ではないのですが「3月14日は何の日」と問えば，生徒は「ホワイトデー」と答えます。では「3.14は」と問えば大抵の答えは「円周率」。『数学の日』の宣伝には好都合で，当日でなくても毎年よく使う話題です。

☆　学校の電話番号は？・・・生徒は答えられません。そういえば子どもたちに「公衆電話のかけ方」を教えるなんて取り組みもあるそうですが・・・。では学校の住所は？・・・住居表示の変更に伴って円周率（伴東三丁目14番1号）になったことを教えます。

つまり，『数学』に繋がりそうなものは多少強引であろうとも何でも使ってみるということです。関連付けが成功すれば，記憶に残って「数学が好きになったり」・「数学を見直したり」するきっかけにならないかなあ・・・という微かな期待という感じでしょうか。

❹　10^n+1 が素数かどうかに関しては，フェルマー数やゼータ関数など同様に私の手には負えそうもありません。ただ，10001,100001,1000001,10000001,100000001,…など個別の数の素因数分解には「数の帝国」
https://ja.numberempire.com/　が便利です。

素因数分解_数の帝国.JPG



❺　素数や暗号に関しては，乱数と暗号の部屋（暗号工房）　http://midarekazu.g2.xrea.com/　が専門家のようです。清宮宏氏は大学の先生なのか在野の研究者なのか正体は全くわかりません。

「Elgamal暗号の暗号化と復号の高速化法（世界最速の公開鍵暗号）と，RSA暗号の復号の高速化法と，Chebyshev多項式による高速公開鍵暗号と，量子コンピュータに対抗できる世界最強の新型公開鍵暗号を開発しました。他に，Mersenne素数を用いた長周期なM系列乱数のコード，ファイル暗号化ソフト「暗GO」，公開鍵暗号化ソフトなどを掲載しました。」
とあり，プログラムなども公開されているのですが，目下のところ私に分かるのかどうかもよく分からないような状態です…。

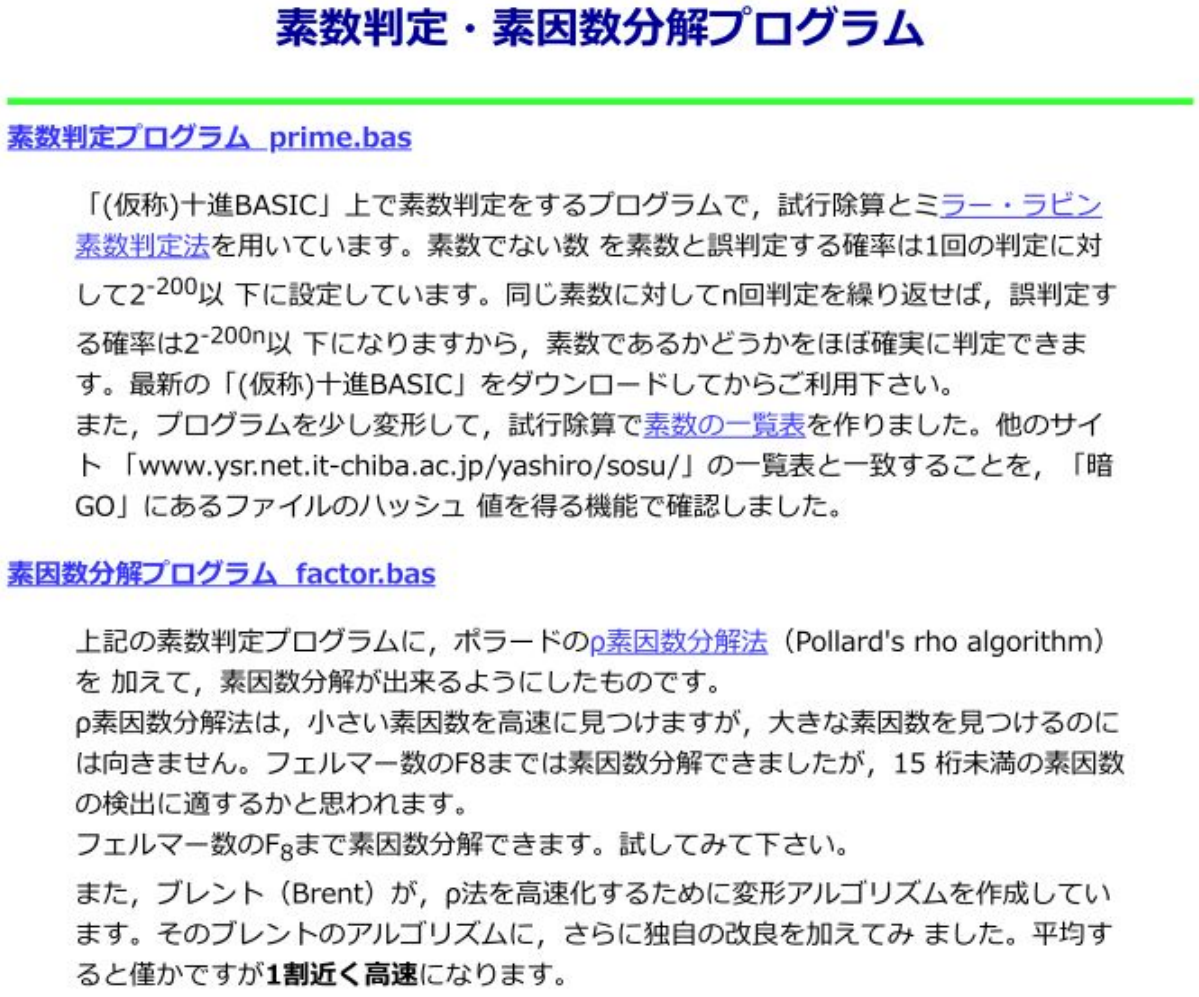
ただ，ページ内には「十進BASIC」を用いた

・素数判定プログラム prime.bas　　や

・素因数分解プログラム factor.bas なども

掲載されており,先にインストールした「十進BASIC」上で試してみることは出来そうです。

素数判定・素因数分解プログラム.JPG



素数判定・素因数分解プログラム

素数判定プログラム　prime.bas

「(仮称)十進BASIC」上で素数判定をするプログラムで，試行除算とミラー・ラビン素数判定法を用いています。素数でない数 を素数と誤判定する確率は1回の判定に対して2^{-200}以 下に設定しています。同じ素数に対してn回判定を繰り返せば，誤判定する確率は2^{-200n}以 下になりますから，素数であるかどうかをほぼ確実に判定できます。最新の「(仮称)十進BASIC」をダウンロードしてからご利用下さい。
また，プログラムを少し変形して，試行除算で素数の一覧表を作りました。他のサイト 「www.ysr.net.it-chiba.ac.jp/yashiro/sosu/」の一覧表と一致することを，「暗GO」にあるファイルのハッシュ 値を得る機能で確認しました。

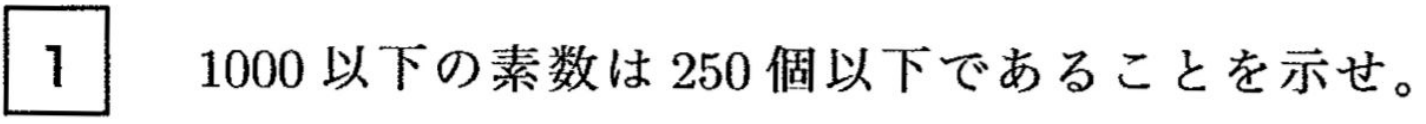
素因数分解プログラム　factor.bas

上記の素数判定プログラムに，ポラードのρ素因数分解法（Pollard's rho algorithm）を 加えて，素因数分解が出来るようにしたものです。
ρ素因数分解法は，小さい素因数を高速に見つけますが，大きな素因数を見つけるのには向きません。フェルマー数のF8までは素因数分解できましたが，15 桁未満の素因数の検出に適するかと思われます。
フェルマー数のF_8まで素因数分解できます。試してみて下さい。
また，ブレント（Brent）が，ρ法を高速化するために変形アルゴリズムを作成しています。そのブレントのアルゴリズムに，さらに独自の改良を加えてみ ました。平均すると僅かですが**1割近く高速**になります。

❻　新しいところでは，2021年一橋大学の数学第1問に次の問題があります。

2021_一橋_第1問_qa_Toshin.pdf

2021_一橋_第1問.JPG



1　1000 以下の素数は 250 個以下であることを示せ。

【数学の話題】

数学の話題