4 つの和集合の個数の小手技

札幌旭丘高校　中村文則

○包除の原理とオイラー関数

<先　生> 本時は和集合の要素の個数の数え方を学習しよう。まずは復習問題です。

> Ex1) 1 から 210 までの自然数で，次の数の個数を求めよ。
> (1) 2 または 3 の倍数。
> (2) 3 または 5 または 7 の倍数。

<まなぶ> ほんとに復習なんだ。いつもは復習でもひねりを入れるのに。
<よしお> 2,3,5,7 の倍数の集合をそれぞれ A, B, C, D として考えるといいかも。2 の倍数の集合の個数は，$n(A)$ と表されるから記述はしやすくなるよ。
<アリス> 例えば，

$$A=\{2\times1,\ 2\times2,\ 2\times3,\ \cdots\cdots,2\times105\}$$

これから，$n(A)=105$ と表すことができるということですね。
<先　生> さらに，要素の個数を求めるにはガウス記号を用いるとすっきりする。ガウス記号は覚えているかな。
<かず子> 確か，x を超えない最大の整数を $[x]$ と表すんでしたよね。
<まなぶ> そうそう，なんかまだるっこしい言い方だった。

$$\left[\sqrt{2}\right]=\left[1.41421356\cdots\right]=1\ ,\ \left[\pi\right]=\left[3.141592\cdots\right]=3$$

この記号は，数の小数部分を切り捨てるだけのことなのに。だから，$n(A)=\left[\dfrac{210}{2}\right]=\left[105\right]=105$ になる。
<アリス> 同じように，集合 B,C,D の要素の個数は次のようになります。

$$n(B)=\left[\frac{210}{3}\right]=70\ ,\ n(C)=\left[\frac{210}{5}\right]=42\ ,\ n(D)=\left[\frac{210}{7}\right]=30$$

<よしお> でも(1)の 2 または 3 の倍数の個数はこれだけではだめだった。
2 の倍数の中にある 3 の倍数，3 の倍数の中にある 2 の倍数が 2 重にカウントされている。
<かず子> 6 の倍数のことよね。それを求めると，

$$n(A\cap B)=\left[\frac{210}{2\cdot3}\right]=35$$

2 または 3 の倍数の個数は $n(A\cup B)$ のことだから，

$$\begin{aligned}n(A\cup B)&=n(A)+n(B)-n(A\cap B)\\&=105+70-35=140\end{aligned}$$

<まなぶ> (2)はもう少し複雑だ。$n(B)$，$n(C)$，$n(D)$ の個数を求めてから，3 の倍数の中の 5 の倍数，5 の倍数の中の 3 の倍数のように 2 重にカウントしているものを抜き去る。

$$n(B\cap C)=\left[\frac{210}{3\cdot5}\right]=14\ ,\ n(B\cap D)=\left[\frac{210}{3\cdot7}\right]=10\ ,\ n(C\cap D)=\left[\frac{210}{5\cdot7}\right]=6$$

でも，引いた部分をみると B, C, D との共通部分はどれも 2 つずつ引いているから，引き過ぎ。
だから 1 つずつ戻すために次を加える。

$$n(B\cap C\cap D)=\left[\frac{210}{3\cdot5\cdot7}\right]=2$$

以上より，

$$\begin{aligned}n(B\cup C\cup D)&=n(B)+n(C)+n(D)-n(B\cap C)-n(B\cap D)-n(C\cap D)+n(B\cap C\cap D)\\&=70+42+30-(14+10+6)+2\\&=114\end{aligned}$$

これでいいと思うけど，いつものトラップが仕まれている歪んだ問題ではない。だから，まだこの後に先生は何か企んでいるはずだ。

<かず子> 人を疑ってかかるそのまなぶの性格の方が私には歪んでいるように見えるわ。
<先　生> そうフォローされるとちょっといいにくくなるのだけど，実は問題の続きがある。

> Ex1) 1 から 210 までの自然数で，次の数の個数を求めよ。
> (3) 2 または 3 または 5 または 7 の倍数

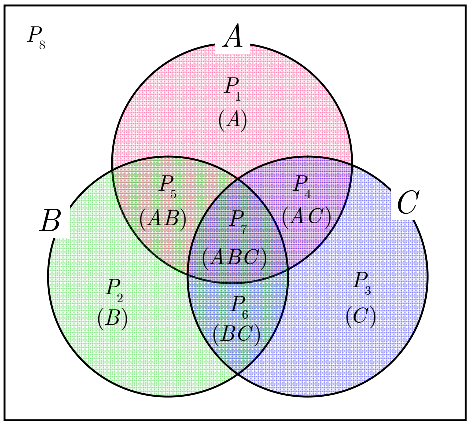
<まなぶ> ほらっ, 僕の言ったとおりだ。問題が 100 以下ではなく 210 以下って中途半端な数なのがなんか怪しかったんだ。先生を見くびってはいけない。先生を一番理解しているのは僕ってことだ。
<かず子> それ，誉め言葉になってないよ。まあ，確かにそのまま終わらせるわけはないわね。
<アリス> そのまま終わらせることはない性格は褒め言葉なのですか。
<先　生> おほん，そのへんにしよう。それでは(3)の問題を考えてごらん。
<よしお> たぶん，3 つの集合と同じように考えて，重なっている集合の個数を引いたり足したりすることは予想できるけど複雑すぎますね。
<先　生> それでは 3 つの集合の場合でもう一度復習をしてみようか。
3 つの集合 A, B, C は右のベン図のように 8 つの集合，

$P_1,\ P_2,\ P_3,\ \cdots\cdots, P_8$

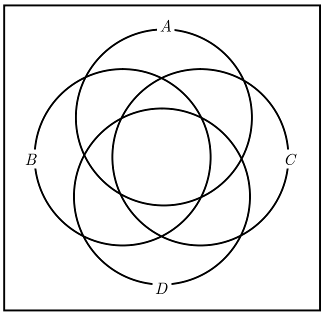
に分割できる。そのそれぞれは，集合 A, B, C またはその補集合の交わりで表される。例えば，

$P_1 = A \cap \overline{B} \cap \overline{C}$ ， $P_5 = A \cap B \cap \overline{C}$ ， $P_7 = A \cap B \cap C$

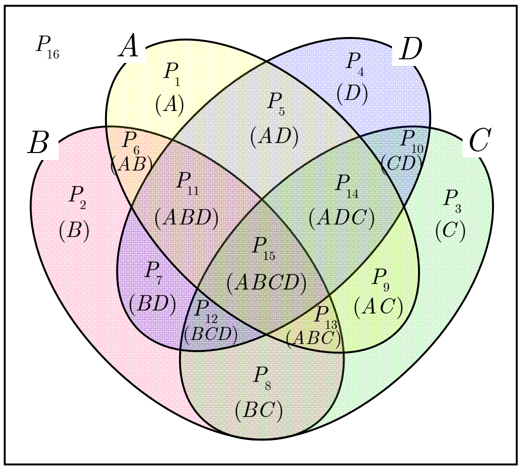
という具合だ。だから，集合 $A \cup B \cup C$ の要素の個数は，集合 P_1 から P_7 までの要素の個数の和になっている。集合 P_1 から P_7 の括弧内の文字は何を表しているか分かりますね。



<かず子> 記載のある文字は含み，記載のない文字は含まないということです。例えば，(ABC)は集合 A，集合 B，集合 C の 3 つを含み，(AB)は集合 A と集合 B は含み，集合 C は含まない。
<先　生> そうです。集合の要素の個数は，切り離したこれらのピースをジグソーパズルのように組合せることなんだ。ではこの方法で 4 つの集合 A, B, C, D のベン図はどのように書けるだろうか。
<アリス> 3 つの集合 A，B，C のベン図の下の方に，集合 D を入れるととても綺麗に書けると思います。



<よしお> 一見，バランスよく集合は配置されているようにみえるけど，分けられる部分の集合は 14 個しかないよ。
<アリス> 14 個ではだめなのですか。
<よしお> 3 つの集合 A，B，C は 8 つの部分の集合に分けられていた。それは 2 つの集合 A, B で分けられる 4 つの部分にもうひとつの集合 C を加えると，それぞれがまた 2 つに分割されて 8 つになるからだよ。これから，3 つの集合で分けられる 8 個の部分は，16 個に分けられなければならない。だから 2 つ足りないんだ。
<まなぶ> なるほど。では何が抜けているのだろう…あっ，分かった。
2 つの集合の重なりをみると，(AB)，(AC)，(BD)，(CD)はあるけど，(BC)はない。
<かず子> そうか。集合 B と C のように向い合っている円(集合)の部分がない。だから，(AD)もないということになります。
<アリス> (AB)のように隣り合っている関係と(AD)の向かい合っている関係が混在していては駄目ということですね。でもそうすると 4 つの集合がみな隣り合うような配置が必要になるけどそんな図を書くことはできるのでしょうか。
<先　生> 結論を言うと不可能なんだ。
<まなぶ> 酷い。書けるだろうかと聞いていながら書けない。かず子，これが先生の本性なんだよ。
<先　生> ちょっと言い方が不適切だった。集合を円として表すことでは無理ということだ。でも右のように合同な 4 つの楕円にするとどの 2 つの集合も隣り合うように配置することができる。



<かず子> 本当だ。みな隣り合っている。そして分けられる部分の個数は 16 個で，集合の重なりは最大 4 つになっている。
<アリス> 1 つの集合のみのピースは $P_1 \sim P_4$ の 4 つ。
2 つの集合は $P_5 \sim P_{10}$ の 6 つ。3 つの集合は $P_{11} \sim P_{14}$ の 4 つ。
そして 4 つの集合は P_{15} の 1 つです。外側の P_{16} を加えると，

$(4+6+4+1)+1=16$

確かに 16 個の集合があります。
<よしお> そうか。これは 4 つの集合の組合せなんだ。
<まなぶ> どういうこと。

<よしお> 4つの集合A，B，C，Dから2つの集合が交わる場合の選び方は ${}_4C_2 = 6$ のように考えればいい。

<まなぶ> 3つの集合，4つの集合が交わる場合，それに1つの集合だけの場合，どの集合も選ばない場合を含めると，

$${}_4C_0 + {}_4C_1 + {}_4C_2 + {}_4C_3 + {}_4C_4 = 2^4 = 16$$

こういうことか。

<かず子> 4つの集合がバランスよく配置されていることもこの式から分かるわ。

<先　生> いいところに気が付いたね。どの集合もその交わりは均等に配置されているからいえることなんだ。

3つの集合の場合でも，

$${}_3C_0 + {}_3C_1 + {}_3C_2 + {}_3C_3 = 2^3 = 8$$

となっている。そしてこの組み合わせから3つの集合の和の個数を調べることができる。

まず，視覚的にイメージしやすいようにしてみよう。

3つの集合A, B, Cを3枚の紙と考える。2枚を重ねると重なる部分ができる。例えばAとBの紙が重なっている部分が集合 $A \cap B$ になる。集合A, B, Cの紙を3枚重ねると $A \cap B \cap C$ であり，これは3つの集合 $A \cap B$, $B \cap C$, $C \cap A$ の重なりの部分とみることができる。

すなわち，集合Aについてみると，その上に $A \cap B$ や $A \cap C$ が重なり，その2つの上には $A \cap B \cap C$ が重なっているということだ。このように，「交わり」は「重なり」とみることにしよう。「重なり2」は2つの集合の重なり，「重なり3」は3つの集合の重なりとする。したがって「重なり1」は重なりのない集合A, B, Cを表す。

これを先ほどのベン図で具体的に示すと次のようになる。

<重なり1>	A	B	C	$\Rightarrow {}_3C_1 = 3$
<重なり2>	$A \cap B$	$B \cap C$	$C \cap A$	$\Rightarrow {}_3C_2 = 3$
<重なり3>		$A \cap B \cap C$		$\Rightarrow {}_3C_3 = 1$

この重なりが1になるように加除をして調整したものが，まなぶが先ほど解いた方法ということだ。

まなぶ，重なりをみて一度説明してごらん。

<まなぶ>　3つの<重なり1>の集合の上には3つの<重なり2>の集合が載っているからこれを除いて重なり1にする。

でも，<重なり2>の上に載っている<重なり3>の集合は引きすぎてなくなるから，<重なり3>を1枚加える。

<先　生> そうだね。その加除の流れをまとめると次のようになる。

<重なり1>	A	B	C	$\Rightarrow {}_3C_1 = 3$
<重なり2>	$A \cap B$	$B \cap C$	$C \cap A$	$\Rightarrow {}_3C_1 - {}_3C_2 = 0$
<重なり3>		$A \cap B \cap C$		$\Rightarrow ({}_3C_1 - {}_3C_2) + {}_3C_3 = 1$

<アリス> <重なり3>のところの組合せは，きれいな式になっていますね。

<よしお> 2つの集合の場合でも，<重なり2>で現れる式は， ${}_2C_1 - {}_2C_2 = 1$ となる。

ということは，4つの集合でも同じようにできるのではないでしょうか。

<先　生> 4つの集合のベン図をみてやってみてごらん。

<かず子> <重なり1>の上にある<重なり2>，その上にある<重なり3>，そしてその上にある<重なり4>を調整するということですね。試しに加除を繰り返してみます……。本当だ，最後はすべての重なりが1になる。

<重なり1>	A	B	C	D			$\Rightarrow {}_4C_1 = 4$
<重なり2>	$A \cap B$	$A \cap C$	$A \cap D$	$B \cap C$	$B \cap D$	$C \cap D$	$\Rightarrow {}_4C_1 - {}_4C_2 = 4 - 6 = -2$
<重なり3>	$A \cap B \cap C$	$A \cap B \cap D$	$A \cap C \cap D$	$B \cap C \cap D$			$\Rightarrow ({}_4C_1 - {}_4C_2) + {}_4C_3 = -2 + 4 = 2$
<重なり4>			$A \cap B \cap C \cap D$				$\Rightarrow ({}_4C_1 - {}_4C_2 + {}_4C_3) - {}_4C_4 = 2 - 1 = 1$

<先　生> このように加除を繰り返して重なりを調整する方法を，「含除の原理」という。

そして，これから4つの集合A, B, C, Dの和集合の個数を求める公式が得られる。

<アリス>　わたし，やってみます。

$$\begin{aligned} n(A \cup B \cup C \cup D) &= n(A) + n(B) + n(C) + n(D) \\ &\quad - \Big(n(A \cap B) + n(A \cap C) + n(A \cap D) + n(B \cap C) + n(B \cap D) + n(C \cap D)\Big) \\ &\quad + \Big(n(A \cap B \cap C) + n(A \cap B \cap D) + n(A \cap C \cap D) + n(B \cap C \cap D)\Big) \\ &\quad - n(A \cap B \cap C \cap D) \end{aligned}$$

これでいいでしょうか。

<まなぶ> そのとおりだと思う。でも計算するときは加除を繰り返せばいいだけだから公式はあまり必要ないよね。

<先　生> 確かにまなぶがいうように，いつものまなぶ流省エネ法の方が何枚重ねでもできるから効率的といえる。
<まなぶ> このご時世，省エネは軽んじてはいけないということ。
<かず子> まなぶがいうと説得力はない。でもまあこの方法で解いてみます。すでに幾つかの集合の個数は求めているのでこちらも省エネで再利用します。<重なり 1>の要素の個数は次の通りです。

$$n(A)=\left[\frac{210}{2}\right]=105\,,\ \ n(B)=\left[\frac{210}{3}\right]=70\,,\ \ n(C)=\left[\frac{210}{5}\right]=42\,,\ \ n(D)=\left[\frac{210}{7}\right]=30$$

次に<重なり 1>の上に載っている<重なり 2>の個数を求めます。

$$n(A\cap B)=\left[\frac{210}{2\cdot 3}\right]=35\,,\ \ n(A\cap C)=\left[\frac{210}{2\cdot 5}\right]=21\,,\ \ n(A\cap D)=\left[\frac{210}{2\cdot 7}\right]=15$$

$$n(B\cap C)=\left[\frac{210}{3\cdot 5}\right]=14\,,\ \ n(B\cap D)=\left[\frac{210}{3\cdot 7}\right]=10\,,\ \ n(C\cap D)=\left[\frac{210}{5\cdot 7}\right]=6$$

ふう，結構たいへん。
<アリス> バトンタッチします。次は<重なり 3>ですね。

$$n(A\cap B\cap C)=\left[\frac{210}{2\cdot 3\cdot 5}\right]=7\,,\quad n(A\cap B\cap D)=\left[\frac{210}{2\cdot 3\cdot 7}\right]=5\,,$$

$$n(A\cap C\cap D)=\left[\frac{210}{2\cdot 5\cdot 7}\right]=3\,,\ \ n(B\cap C\cap D)=\left[\frac{210}{3\cdot 5\cdot 7}\right]=2$$

どうにかできました。最後は<重なり 4>です。

$$n(A\cap B\cap C\cap D)=\left[\frac{210}{2\cdot 3\cdot 5\cdot 7}\right]=1$$

<まなぶ> この加除を繰り返せばいいということか。だから，

$$(105+70+42+30)-(35+21+15+14+10+6)+(7+5+3+2)-1$$
$$=247-101+17-1=162$$

できた。面白いね。含除というのは加除のことだと思うけど，要素の個数を調べるための「ほじょの原理」っ感じ。
<かず子> うま味だけ独り占めしてなに悦に入ってのよ。わたしとアリスが計算したその補助の部分が大変なのよ。
<よしお> 集合の個数がもっと増えるとさらに計算は大変になる。これをさらに省エネで求める方法はないのだろうか。
<先　生> なんか省エネが伝染しちゃったね。でもちょっと考えてみようか。
<まなぶ> あるの？。生徒に苦労させて楽しんでいない。こういうのを徒労っていうんだよ。
<先　生> 「ほじょの原理」に比べいい例えだ。話を戻そう。まず 2 つの集合で考えてみる。
自然数 n が異なる 2 つの素数 a,b を因数にもつとき，n 以下の a または b の倍数の個数を求める。
n は，a，b，ab の倍数だから，

<重なり 1>の個数は $\dfrac{n}{a}+\dfrac{n}{b}$　　<重なり 2>の個数は $\dfrac{n}{ab}$

よって，

$$\left(\frac{n}{a}+\frac{n}{b}\right)-\frac{n}{ab}=n\left(\frac{1}{a}+\frac{1}{b}-\frac{1}{ab}\right)\qquad\cdots(*)$$

<かず子> 先生，この式だと結局は単純計算になってしまうのでは。
<先　生> このままではそうだ。ここで，式の中の，$\dfrac{1}{a}+\dfrac{1}{b}$ と $\dfrac{1}{ab}$ は，2 数 $\dfrac{1}{a}$ と $\dfrac{1}{b}$ の和と積になっていることに注目。
<まなぶ> 何かいままでの解法とは違った道に進む予感する。
<よしお> 2 数の和と積なのだから，2 次方程式の解と係数の関係を用いるということでしょうか。
<先　生> そのとおり。$\dfrac{1}{a}$ と $\dfrac{1}{b}$ を 2 解とする 2 次方程式を 1 つ求めてごらん。
<アリス> はい。$x^2-\left(\dfrac{1}{a}+\dfrac{1}{b}\right)x+\dfrac{1}{ab}=0$ です。
<先　生> すなわち，左辺は次のように因数分解できる。

$$x^2-\left(\frac{1}{a}+\frac{1}{b}\right)x+\frac{1}{ab}=\left(x-\frac{1}{a}\right)\left(x-\frac{1}{b}\right)$$

この式の x に，適当な数値を入れて(*)を変形できないだろうか。
<かず子> あっ，分かった。$x=1$ を代入すればいいのですね。

$$1-\left(\frac{1}{a}+\frac{1}{b}\right)+\frac{1}{ab}=\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$$

これから，両辺をn倍して整理すると，

$$n\left(\frac{1}{a}+\frac{1}{b}-\frac{1}{ab}\right)=n\left\{1-\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\right\}$$

<よしお> 同じように考えると 3 つの集合の場合もできるということですね。

<先　生> やってみようか。自然数nが異なる 3 つの素数a,b,cを因数にもつとき，n以下の自然数で，a またはb またはcの倍数である個数を求めてみよう。その個数mは次式で得られる。

$$m=\left(\frac{n}{a}+\frac{n}{b}+\frac{n}{c}\right)-\left(\frac{n}{ab}+\frac{n}{ac}+\frac{n}{bc}\right)+\frac{n}{abc}$$

ここで，3 次方程式の解と係数の関係より，

$$x^3-\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)x^2+\left(\frac{1}{ab}+\frac{1}{ac}+\frac{1}{bc}\right)x-\frac{1}{abc}=\left(x-\frac{1}{a}\right)\left(x-\frac{1}{b}\right)\left(x-\frac{1}{c}\right)$$

$x=1$を代入して両辺をn倍すると，

$$m=n\left\{1-\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\right\}$$

さあ，できたね。

<アリス> えっ，たったこれだけの計算式にまとめられてしまうのですか。

ためしに，(2)の 3 または 5 または 7 の倍数の個数を求めてみます。個数をmとすると，

$$m=210\times\left\{1-\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\right\}=210\times\left(1-\frac{2}{3}\times\frac{4}{5}\times\frac{6}{7}\right)=210\times\frac{19}{5\cdot 7}=114$$

ほんと，できちゃいました。

<まなぶ> 同じように考えると 4 つの集合の場合もできるということになる。

210 以下の自然数で，2，3，5，7 の少なくとも 1 つの倍数である数の個数mは,

$$m=210\times\left\{1-\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\right\}=210\times\left(1-\frac{1}{2}\times\frac{2}{3}\times\frac{4}{5}\times\frac{6}{7}\right)=210\times\frac{27}{5\cdot 7}=162$$

簡単だ。徒労の言葉が胸に突き刺さる。なんか妙に腹が立ってきた。

<かず子> あのね。繰り返すけど(3)の地道な計算をしたのは貴方じゃないのよ。

<まなぶ> でも先生，これは 210 が 2,3,5,7 で割り切れるからできるんだよね。ふつうの問題だと 1000 以下の個数とかそういう問題でしょ。そういうときは使えないのでは。

<先　生> その場合は含除の原理で求めることになるけど，この方法でできないか考えてみようか。

Ex2) 1 から 1,000 までの自然数で，2,3,5,7 の少なくとも 1 つの倍数の個数を求めよ。

<まなぶ> できるんですか?，できるんだ!!。また腹が立ってきた。

<先　生> とりあえず，含除の原理で解いてみよう。

<かず子> まなぶが質問したのだから後半の計算はまなぶにしてもらうからね。

まず，<重なり 1>を計算すると，

$$\left[\frac{1000}{2}\right]=500,\ \left[\frac{1000}{3}\right]=333,\ \left[\frac{1000}{5}\right]=200,\ \left[\frac{1000}{7}\right]=142$$

さあ，まなぶ。後はあなたが計算して。

<まなぶ> バトンタッチ，早すぎない。失敗した，質問しなければよかった。

<重なり 2>は,

$$\left[\frac{1000}{2\cdot 3}\right]=166,\ \left[\frac{1000}{2\cdot 5}\right]=100,\ \left[\frac{1000}{2\cdot 7}\right]=71,\ \left[\frac{1000}{3\cdot 5}\right]=66,\ \left[\frac{1000}{3\cdot 7}\right]=47,\ \left[\frac{1000}{5\cdot 7}\right]=28$$

まだあるのか。次は<重なり 3>は,

$$\left[\frac{1000}{2\cdot 3\cdot 5}\right]=33,\ \left[\frac{1000}{2\cdot 3\cdot 7}\right]=23,\ \left[\frac{1000}{2\cdot 5\cdot 7}\right]=14,\ \left[\frac{1000}{3\cdot 5\cdot 7}\right]=9$$

やっと最後だ。<重なり 4>は,

$$\left[\frac{1000}{2\cdot 3\cdot 5\cdot 6}\right]=4$$

あとは加除を繰り返す。

$$\begin{aligned} m &= (500+333+200+142)-(166+100+71+66+47+28)+(33+23+14+9)-4 \\ &= 1175-478+79-4 \\ &= 772 \end{aligned}$$

できた。まあ，計算してみればたいしたことない。もうこれで十分かも。

<よしお>　これを先ほどの方法で求めようとすると，2 と 5 は 1000 の約数だけど，3 と 7 では割り切れないから使えない。どうすればいいのだろうか。

<アリス> あのう，単純かもしれませんが言っていいですか。割り切れるような数にして考えることはできませんか。

<先　生> もう少し詳しく説明してごらん。

<アリス>　1000 の前後の数で，2, 3, 5, 7 のどれでも割り切れる数をみつけるんです。そのあと，残りの数は原始的な方法なんですけど，直接数えて調整するんです。

<かず子> 数える!，なんかアリス，まなぶに感化というか汚染されていない。

<まなぶ> アリスの言うこと分かるよ。さきほどの包除の原理も公式を使うよりは加除を繰り返した方がよかった。簡単なものにまで大げさな公式を使う必要はないと思うな。

<先　生> その通り。簡単に求めることができる方法があれば，それを利用することを考えてみる。郷に入れば郷に従えということだ。その方法でやってみよう。1,000 の前後の数で，2,3,5,7 で割り切れる数を探してごらん。

<よしお>　先ほどの 210 は 2,5,7,9 で割り切れる数でしたからこの数をリユースできますね。210 の倍数で 1000 に近い数をみつければいい。

<かず子>　$210\times4=840$ はどうかしら。

<まなぶ> $210\times5=1050$ の方がもっと近いよ。

<先　生> $1050=2\cdot3\cdot5^2\cdot7$ ということだね。

それでは，1050 以下で 2,3,5,7 の少なくとも 1 つの倍数の個数を求めてみよう。

<アリス> これは簡単です。その個数を m とすると，

$$m=1050\times\left\{1-\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\right\}=1050\times\frac{27}{5\cdot7}=810$$

<まなぶ> 1,000 以下を求めるのだから，不要な 1,001～1,050 にある 2, 3, 3, 5 の倍数の個数を除けばいいということだ。

<かず子>　調べる数が 50 個もある。けっこう大変ではないですか。

<先　生> ぜんぶ調べる必要はない。目視でカウントできる数がある。

<よしお> 偶数ですね。25 個あるのはすぐに分かります。結局，1001 から 1050 の間にある 25 個の奇数を調べればいい。

<先　生> 数えやすいように 25 個の奇数を 5 個ずつまとめて書き抜き，左下図のように 5 行 5 列の表を作る。この中から，3, 5, 7 の倍数を探してみてごらん。

<アリス> やってみます。まず，3 の倍数ですね。3 の倍数は「各位の数の和が 3 の倍数」になっているから，最初に現れる数は 1005。次は，1011, 1017…。あれ，2 つ置きに出現しています。同じ間隔で現れるのですね。

<まなぶ> 5 の倍数は左から 3 つめの列にすべて現れている。

<かず子> あとは 7 の倍数ね。7 の倍数の判定方法があったわよね。何だったかしら。

<よしお>　数を下の位から 3 桁ずつ区切って 3 桁の整数にし，それらの数を交互に加除をしていき計算した値が 7 の倍数になっていればいい。

<かず子> そうだった。なんか，含除の原理と似ているわ。そうすると，1,015 は，1 と 015 に区切るから $15-1=14=7\times2$ 。ためしにこれも 6 つ置きに調べてみると，1,029，1,043。やっぱり 7 の倍数になっているわ。

<よしお> かず子，1,015 の前に 6 つ置いた 1,001 もそうだよ。

<かず子> えっ，そうなの。1,001 は，1 と 001 だから差は 0。そうか，0 も 7 の倍数なのね。これですべてね。

そうすると，右下表から，3 または 5 または 7 の倍数は 13 個。これに偶数の 25 個を加えて 38 個。先ほどの 1,050 以下の個数 m から引くと，

$$m-38=810-38=772$$

含除の原理で求めた値と一致したわ。こちらの解法の方が良さそうだわ。

1001	1003	1005	1007	1009
1011	1013	1015	1017	1019
1021	1023	1025	1027	1029
1031	1033	1035	1037	1039
1041	1043	1045	1047	1049

⇒

1001	1003	**1005**	1007	1009
1011	1013	1015	**1017**	1019
1021	**1023**	1025	1027	**1029**
1031	1033	**1035**	1037	1039
1041	1043	1045	**1047**	1049

⇒

1001	1003	**1005**	1007	1009
1011	1013	**1015**	**1017**	1019
1021	**1023**	**1025**	1027	**1029**
1031	1033	**1035**	1037	1039
1041	1043	**1045**	**1047**	1049

⇒

1001	1003	**1005**	1007	1009
1011	1013	**1015**	**1017**	1019
1021	**1023**	**1025**	1027	**1029**
1031	1033	**1035**	1037	1039
1041	**1043**	**1045**	**1047**	1049

<先　生> このように公式だけで解こうとするのではなく地道に数え上げることを併用し，緩急組み合わせることも大事なことなんだ。それではこの方法でもう一題解いてみよう。

Ex3) 1 から 10,000 までの自然数で，2，5，7，11，13 の少なくとも 1 つの倍数である数の個数を求めよ

<まなぶ>　5 つの和集合なの。なんでこんなマニアックで非常識な問題だすのかな。包除の原理で解けなんて言わないでよ。

<よしお>　さすがにこれは無理だよ。2 つの集合の組合せは ${}_5C_2 = 10$ 通りで，これだけでも大変。全部で $2^5 = 32$ 通りの割り算が必要になる。

<アリス> 5 つの数を因数にもつ 10,000 に近い数を探すしかないということですね。

まず，この 5 つの数の積を計算してみます。

$$2\times 5\times 7\times 11\times 13 = 10010$$

なんだ，10,000 にすごく近い数です。だから 10,010 以下の倍数を求めて，必要ない数を除けばいい。

1 から 10,010 で 2，5，7，11，13 の倍数の個数 m は

$$\begin{aligned} m &= 10010\times\left\{1-\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\right\} \\ &= 10010\times\left(1-\frac{1}{2}\times\frac{4}{5}\times\frac{6}{7}\times\frac{10}{11}\times\frac{12}{13}\right) \\ &= 10010\times\frac{713}{7\times 11\times 13} = 7130 \end{aligned}$$

<かず子> あとは，10,001〜10,010 の 10 個の数の中にある 2, 5, 7, 11, 13 の倍数を除きます。

2 の倍数は 5 個より，奇数を抜き出すと，

10,001　10,003　10,005　10,007　10,009

3 の倍数は 10,005 だけだわ。そしてこれは 5 の倍数にもなっている。

7 の倍数は，3 桁ずつ区切りその差を考える。

10 と 003 は，$10-3=7$ 。だから 7 の倍数で，これしかないわ。

でも，11 と 13 の倍数の判定はどうすればいいのかしら。

<先　生> 実は，これも 7 の倍数の判定法と同じなんだ。3 桁ごとに区切り，加除を繰り返して得られた数が，11 や 13 の倍数になっていればいい。

<まなぶ> へ一っ，面白いな。小さい数から順に計算してみると。

$10-1=9$，$10-3=7$，$10-5=5$，$10-7=3$，$10-9=1$

どれも 11, 13 の倍数にならない。先ほどかず子が調べた 7 の倍数 10,003 以外はないということか。

だから，減じる個数は，$5+1+1=7$ 個。以上より，

$$m-7 = 7130-7 = 7123$$

先生，それなりに考えて出題していたんだね。

<よしお> ちょっと思いついたことがあるんですが。

アリスが計算した式で，$n = 10010$ とおくと，

$$n-m = n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)$$

となりますよね。この左辺は整数 n から 2, 5, 7, 11, 13 のいずれかで割り切れる数を減じたものだから，2, 5, 7, 11, 13 のいずれでも割り切れない数の個数です。そして，n を素因数分解すると，

$$n = 2\cdot 5\cdot 7\cdot 11\cdot 13$$

すなわちこの 5 個以外に n の素因数はありません。このことから，右辺の計算は，10,010 と互いに素である数の個数を求めているのではないでしょうか。

<先　生>　よく気が付いたね。それが本時のまとめとしてみんなに言いたかったことなんだ。

もう少し，簡単な例で考えみよう。

> Ex4) 30 以下の自然数で 30 と互いに素である数の個数を求めよ。

<先　生> さて，$30 = 2\cdot 3\cdot 5$ だから，互いに素である数は 2 でも 3 でも 5 でも割り切れない数になる。

そこで 30 以下の奇数を抜き出して下表を作る。

ここから 3 の倍数を抜き，さらに 5 の倍数を抜いてみる。

倍　数	1から30までの奇数															割合
3 の倍数	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	5/15
5 の倍数	1		5	7		11	13		17	19		23	25		29	2/10
互いに素	1			7		11	13		17	19		23			29	

この表をよくみてみよう。30 以下の自然数で偶数は $\frac{1}{2}$ の割合だから，奇数も $\frac{1}{2}$ の割合の 15 個ということを示している。次に 3 の倍数は 5 個あるけどこれは奇数 15 個のうち $\frac{1}{3}$ の割合ということだ。だから，15 個の $\frac{2}{3}$ の割合，すなわち 10 個が 3 の倍数でないということだ。ではこの 10 個に対して 5 の倍数はどうなっているだろう。

<アリス> 10 個の中で 5 の倍数は 2 個しかありません。だから $\dfrac{1}{5}$ の割合ということですね。したがって，10 個の $\dfrac{4}{5}$ である 8 個が 5 の倍数ではないということになります。
<よしお> そうか，30 個に数に対して，素因数の倍数にならない割合を求めていけばいいんですね。

$$30\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=30\times\frac{1}{2}\times\frac{2}{3}\times\frac{4}{5}=8$$

これで納得できました。
<先　生> このように，n 以下の数で n と互いに素である自然数の個数を得る関数を，「オイラーの関数」といい，$\varphi(n)$ で表す。自然数 n を素因数分解して，$n=a^p b^q c^r d^s$ となるときは，次のようになる。

$$\varphi(n)=n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\left(1-\frac{1}{d}\right)$$

先ほどの問題は，$\varphi(30)=8$ ということだ。次を求めてみよう。

Ex5) 次の値を求めよ。
(1) $\varphi(23)$　(2) $\varphi(60)$　(3) $\varphi(1001)$

<よしお> (1)の 23 は素数だから，23 と互いに素である数は 1 しかない。だから互いに素である数の個数は 22 個です。でもこれをオイラーの関数で求めてみると，

$$\varphi(23)=23\times\left(1-\frac{1}{23}\right)=22$$

こういうことですね。
<先　生> そうだね。機械的に公式を用いるのでなく，その公式の意味を理解するようにしよう。
<アリス> (2)は，$60=2^2\cdot3\cdot5$ だから，素因数は $2, 3, 5$ ね。だから，

$$\varphi(60)=60\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=60\times\frac{1\cdot2\cdot4}{2\cdot3\cdot5}=16$$

これは数えたくはないですね。
<まなぶ> (3)は直接数えるのは絶対無理。だいたいこれ，素因数分解できるの。
<かず子> この数 1,001 は先ほど問題で調べたでしょ。3 桁毎に分けた 2 数の差は 0 になっているよ。
<まなぶ> ということは，7 の倍数で，さらに 11，13 の倍数ということだ。素因数分解すると，

$$1001=7\times11\times13$$

これから，

$$\varphi(1001)=1001\times\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)=1001\times\frac{6\cdot10\cdot12}{7\cdot11\cdot13}=720$$

<よしお> 包除の原理から得られた公式は，オイラー関数が背景にあったのですね。
<先　生> オイラー関数は，自然数 n のすべての素因数に対しての公式だ。でも包除の原理で考えた方法は，いくつかの素因数に対して成立している。だから大事なことは，公式そのものより公式の意味を理解してそれを活用できるようにすることなんだ。
<まなぶ> オイラー様様。問題を解くときは「おいらがほじょする」ってことだよね。
<かず子> なに，そのおやじギャグならぬ小砂利ギャグは。活用の意味をまるで理解してない。言葉を活用してまなぶを表現するなら，さしずめ，「おー，いらねー。放除しよう」ってことだわ。

あとがき

2021 年度，センター試験は大学入学共通テストに衣替えをしました。試験内容は，従来のセンター試験とそれほど傾向は変わっていない教科もありました。しかし数学では，試行調査問題，モデル問題で示された思考力，判断力，表現力を問う傾向が踏襲され，太郎と花子の 2 人の古風ゆかしい名前のナビゲータにより誘導の形式で出題されました。見方によっては過度の誘導により思考は固められ,判断はナビゲータに委ねられ,そして式の表現は制約されてしまったかもしれませんが。

問い　$\tan 1^\circ$ は有理数か

2006 年度，京都大学の後期の問題です。受験史上，もっとも短い設問の問題として知られています。$\tan 1^\circ$ は無理数ですが，有理数でないことを判断させ，どのような方法で解くか思考を巡らせ，立てた方針を表現していく。これぞまさに 3 つの力を養う良問といえるでしょう。それが共通テストでは設問の文章量が増え，読むことに多くの時間が費やされ，残りの短い時間は，太郎と花子の言葉の分析で終わってしまったような印象を受けます。これからの共通テストは問題の分析よりも言葉の分析が中心となってしまうのでしょうか。
個別試験でも，私立大学では 3 つの力を問う出題があり，ソーシャルディスタンスを満たす距離の確率などまるで共通テ

ストと見間違えるような問題もありました。そうした中で，今年度は整数の性質に関わる問題がずいぶん多く出題されました。新学習要領では，「整数の性質」は数学Aの３領域の１つである「数学と人間の活動」に追いやられ，二進法，ユークリッドの互除法の簡単な話題に限定され，不定方程式は削除されます。「数学と人間の活動」が共通テストの出題範囲になる可能性は低く，結局は高校数学から削除ということになってしまいそうです。だから，出題者はそのことを考えてストック問題を出題したかというと，そうではないと思います。３つの力を養うには「整数の性質」は適材の分野なのです。

問い 3^n-2^n が素数ならば n も素数であることを示せ。

今年度の京都大学の問題です。，解法の指針を定め，公式ツールを引き出す過程はとても面白いものです。

問い 1000 以下の素数は 250 個以下であることを示せ。

こちらは，一橋大学の問題で，第１問で出題されたので受験生は戸惑ったかもしれません。
そして，この問題が今回の小手技のモデル(ネタ)となっています。そこで，問題の解答を考えながら本文のまとめをすることにします。
この問題の解法フローチャートのスタートは，直接数えるかどうかで，2 つに分岐できます。以下，考えてみましょう。

Ⅰ．直接数えない場合

直接数えないのであれば，合成数を求めで，全体 1000 から引けばいいことになります。
合成数の素因数 p は,

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad 13,\cdots$$

となります。すなわち p の倍数の集合の個数を求めるということです。
しかし，学習指導要領では集合の和の個数は３つまでしか扱わないので，まず，2, 3, 5 の倍数の個数を求めましょう。
2, 3, 5 の倍数の集合をそれぞれ A，B，C とします。

$$n(A)=\left[\frac{1000}{2}\right]=500\,,\quad n(B)=\left[\frac{1000}{3}\right]=333\,,\quad n(C)=\left[\frac{1000}{5}\right]=200$$

$$n(A\cap B)=\left[\frac{1000}{2\cdot 3}\right]=166\,,\quad n(A\cap C)=\left[\frac{1000}{2\cdot 5}\right]=100\,,\quad n(B\cap C)=\left[\frac{1000}{3\cdot 5}\right]=66$$

$$n(A\cap B\cap C)=\left[\frac{1000}{2\cdot 3\cdot 5}\right]=33$$

$$\therefore\qquad n(A\cup B\cup C)=(500+333+200)-(166+100+66)+33=734$$

この中には素数 2, 3, 5 も含まれるので，素数候補は,

$$1000-(734-3)=269$$ （1 は素数でないのでこれも除くと 268)

残念ながら，250 個を超えてしまいます。
そこで，7 の倍数の集合 D を加えて，4 つの集合の和の公式で再計算しなければいけません。
教科書では扱わないので，補題として証明することになります。

$A\cup B\cup C\cup D=(A\cup B\cup C)\cup D$ より，

$$\begin{aligned}n(A\cup B\cup C\cup D)&=n(A\cup B\cup C)+n(D)-n((A\cup B\cup C)\cap D)\\&=n(A)+n(B)+n(C)+n(D)-n(A\cap B)-n(A\cap C)-n(B\cap C)+n(A\cap B\cap C)\\&\quad-n((A\cup B\cup C)\cap D)\end{aligned}$$

$(A\cup B\cup C)\cap D=(A\cap D)\cup(B\cap D)\cup(C\cap D)$ であることから,

$$\begin{aligned}n((A\cap D)\cup(B\cap D)\cup(C\cap D))&=n(A\cap B)+n(A\cap C)+n(A\cap D)\\&\quad-n(A\cap B\cap C)-n(A\cap B\cap D)-n(A\cap C\cap D)\\&\quad+n(A\cap B\cap C\cap D)\end{aligned}$$

まとめると公式が得られます。それでは，1000 以下で 2, 3, 5, 7 の少なくとも１つ倍数である数の個数を求めてみましょう。
2, 3, 5, 7 の倍数の集合をそれぞれ A，B，C，D とします。

$$n(A)=\left[\frac{1000}{2}\right]=500\,,\quad n(B)=\left[\frac{1000}{3}\right]=333\,,\quad n(C)=\left[\frac{1000}{5}\right]=200\,,\quad n(D)=\left[\frac{1000}{7}\right]=142$$

$$n(A\cap B)=\left[\frac{1000}{2\cdot 3}\right]=166\,,\quad n(A\cap C)=\left[\frac{1000}{2\cdot 5}\right]=100\,,\quad n(A\cap D)=\left[\frac{1000}{2\cdot 7}\right]=71$$

$$n(B\cap C)=\left[\frac{1000}{3\cdot 5}\right]=66\,,\quad n(B\cap D)=\left[\frac{1000}{3\cdot 7}\right]=47\,,\quad n(C\cap D)=\left[\frac{1000}{5\cdot 7}\right]=28$$

$$n(A\cap B\cap C)=\left[\frac{1000}{2\cdot 3\cdot 5}\right]=33\,,\quad n(A\cap B\cap D)=\left[\frac{1000}{2\cdot 3\cdot 7}\right]=23\,,\quad n(A\cap C\cap D)=\left[\frac{1000}{2\cdot 5\cdot 7}\right]=14$$

$$n(B\cap C\cap D)=\left[\frac{1000}{3\cdot 5\cdot 7}\right]=9\,,\quad n(A\cap B\cap C\cap D)=\left[\frac{1000}{2\cdot 3\cdot 5\cdot 7}\right]=4$$

以上より，公式に代入して

$$\begin{aligned} n(A\cup B\cup C\cup D) &= (500+333+200+142)-(166+100+71+66+47+28) \\ &\quad +(33+23+14+9)-4=772 \end{aligned}$$

この 772 個の中には，2, 3, 5, 7 の素数も含まれているから，合成数は 768 個です。

したがって，1000 以下の素数候補は，$1000-768=232$ より，素数は 250 個以下になります。

ただ，これでは 3 つの集合の分配法則を用いることになり，これも現教育課程では範囲外なのです。もちろん，含除の原理も使うことはできません。そこで，本文でやったように「直接数える」ことで残りを調べてみましょう。

2, 3, 5 のいずれの倍数でもない素数候補は 269 個でした。だから，7 以上の素数から 2 数以上を選び，その積で得られる合成数の個数が 19 個以上あればいいことになります。7 以上の素数を抜き出すと，

7, 11, 13, 17, 19, 23, 29, 31, 37, 41, $\cdots$

ここで，7 から 29 までの 7 個から異なる 2 数を選ぶ場合の数は ${}_7C_2=21$ です。これらの中で最大の合成数は $23\times 29=667$ より 1,000 以下なので，この 29 個で条件を満たしています。

最も少ない個数の素数で合成数を作るならば，7 から 23 までの 6 個の素数を重複(平方数)を許してを 2 つ選びます。その場合の数は ${}_6H_2={}_7C_2=21$ で最大の合成数は $23^2=529$ より満たしています。このように適当に 2 つ以上の素数の積をとることで幾らでも必要な個数の合成数を探すことは可能なのです。それを 4 つの集合の和の公式を持ち出し大仰に構えて計算しようとすると目標を見失ってしまいます。こういう柔軟な発想が 3 つの力で本来養うものなのではないでしょうか。

なお，n 個の集合の和の公式は，数学的帰納法で求めることができます。それは前述の 4 つの集合の変形が 3 つの集合の公式を用いて導かれていることから分かります。それを本文の包除の原理では，集合の重なりで説明していますが，n 個の集合の個数の和でも成立することを示しましょう。

まず分割される部分集合の個数は次で与えられます。

$${}_nC_0+{}_nC_1+{}_nC_2+{}_nC_3+\cdots\cdots+{}_nC_{n-1}+{}_nC_n=2^n$$

これらの 2^n 個に分割された集合の重なりを調べます。例えば，<重なり 1>は ${}_nC_1=n$ で選べます。その上に載る部分集合を，加除を交互に繰り返して調整します。最終的に<重なり 1>になるようにするために，次の式を証明します。

$${}_nC_1-{}_nC_2+{}_nC_3-{}_nC_4+\cdots\cdots+(-1)^{n-1}{}_nC_n=1$$

二項定理より，　$(x+1)^n=\sum_{k=0}^{n}{}_nC_kx^k=1+\sum_{k=1}^{n}{}_nC_kx^k$

$x=-1$ を代入すると，　$0=1+\sum_{k=1}^{n}{}_nC_k(-1)^k$　　これより，$1=-\sum_{k=1}^{n}{}_nC_k(-1)^k=\sum_{k=1}^{n}{}_nC_k(-1)^{k-1}$

Ⅱ．直接数える場合

直接数えるには，「エラトステネスの篩」を用いるのがもっとも単純な方法でしょう。これは新学習指導要領では「数学と人間の活動」の中でその歴史も触れて扱われるかもしれません。また，コンピュータの活用の一例として示すことも考えられます。表計算 Excel の VBA でプログラムを書いてもそれほど難しくはなく，実際にプログラムを走らせて，素数の個数は正確には 168 個になることを確認させることも効果的です。

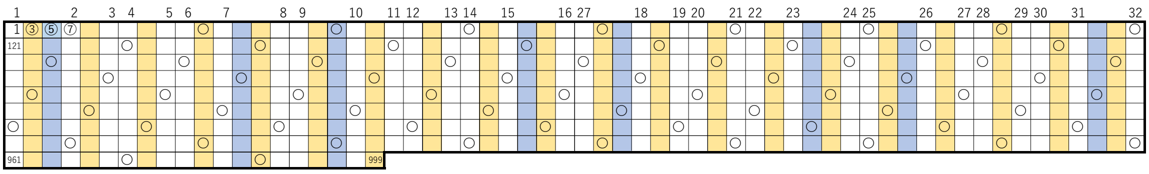
エラトステネスの篩を知っている受験生で，実際に書き抜いてふるい落とし答えを導いた受験生はいたのでしょうか。

1000 までの自然数を抜き出すのは大変なので，本文で示したように奇数 500 個で考えます。3, 5, 7 の倍数だけを調べるのならば，105 個ずつ並べていくときれいに消せますが，3 と 5 だけでみて 60 個ずつ 9 行並べます。下表が完成図です。奇数列でも 3 の倍数，5 の倍数は等間隔に現れるので数値を入れる必要はありません。3 または 5 の倍数は下表の塗られているセルになります。表の上に書いてある数字は色が塗られていない列をカウントしたものです。これからその総数は，

$32\times 8+10=266$

これが素数候補になりますが，素数 2, 3, 5 も除かれているので 3 数を加えると 269 個になります。あとはこの素数候補から合成数を抜いていきます。7 の倍数であるセルは○で示しています。7 の倍数もまた規則正しく配置されていることが分かります。この中で色の塗られていない○のついたセル(7 の倍数)が 20 個以上(1 は素数でないから)あれば終了です。

なお，奇数だけで篩にかけて素数を調べるアルゴリズムは，インドのサスヤマンガラムの生徒が考案しており，「サンダラムの篩」といわれています。



1	③	⑤	⑦							○				
		○							○					
	○							○						
○							○							○
						○							○	
					○							○		
				○							○			

それでも表を作るのが面倒な場合は，右のように，(横$3\times5=15$　縦 7)のブロック表を作ります。3 の倍数でも 5 の倍数でもない色の塗られていないセルは，1 つの行に 8 つあります。

$$500=15\times33+5 \quad \cdots①$$

これから，5 つのセルが最後に残り，色の塗られていないセルは 2 つより，

$$8\times33+2=266$$

次に 7 の倍数ですが，○のついたものです。7 の倍数は 7 行で 1 つのサイクルですが，この中にある色の塗られていない○(未カウント)のセルは 7 行で 8 個あります。したがって，このブロック表が 3 つあればいいことになりますが，266 個の中のすべての未カウント(7 の倍数)の個数を求めてみましょう。

$33=7\times4+5$ より①を変形すると，

$$500=15\times7\times4+15\times5+5$$

$3\times5\times7$ の 4 ブロックの未カウントの個数は $8\times4=32$ 個です。残りの 1 ブロックにならない($15\times5+5$)分の未カウントの個数は表より 6 個になります。したがって $8\times4+6=38$ 個が未カウントの総数です。よって，2, 3, 5, 7 のいずれの倍数でもない個数は，

$$266-38=228\ (個)$$

になります。ところで，この問題では素数の個数が 250 個以下を示すので，2, 3, 5, 7 の 4 つの素数の倍数のふるいで求められます。では，素数の個数が 200 個以下の場合は，さらに，7, 11, 13, 17, 13. …と続け，これらの素数の倍数でふるいをかけなければなりません。ではどこまでこれを続ければいいのでしょうか。

たとえば 23 でふるいをかけるとき，その倍数を $23k$ と表します，このとき $k=1, 2, 3, \cdots, 22$ までは，すでにふるいにかけられています。なぜならば，$23k=k\times23$ とすると次のようになるからです。

$23\times2=2\times23$ (2 の倍数)　$23\times21=3\times7\times23$ (3 の倍数)　$23\times19=19\times23$ (19 の倍数)

これから，$k\geqq23$ でふるいをかければいいことになります。

いま 1 から n までの数でエラトステネスのふるいをかけるとき，その最大素数 p のふるいは次を満たします。

$$p\leqq k \quad \cdots① \qquad kp\leqq n \quad \cdots②$$

①の両辺に p を掛けて，　$p^2\leqq kp$　　②より，$p^2\leqq kp\leqq n$

$$\therefore \quad p\leqq\sqrt{n}$$

よって，$n=1000$ のときは，$p\leqq\sqrt{1000}=31.6\cdots$。すなわち $p=31$ がふるいをかける最後の素数になります。

$p=31$ のときは，

$$31\times31=961,\ 31\times32=992\ (2の倍数),\ 31\times33=1023\ (3の倍数)$$

31^2 以外は，すでにふるいにかけられているか 1000 を超えてしまいます。

このようにエラトステネスの篩により理論上は求められるのですが効率的な方法とはいえません。そこでもっと鮮やかに解決する方法として初等整数論の重要な関数であるオイラーの関数(オイラーのトーシェント関数)を利用します。

本文でも述べたようにオイラー関数は，次の式で与えられます。

自然数 n と互いに素である n 以下の自然数の個数 $\varphi(n)$ は，

$$\varphi(n)=\prod_{k=1}^{m}\left(1-\frac{1}{p_k}\right) \qquad (p_k\ はnの素因数)$$

オイラー関数を用いると高速で互いに素である数の個数を求めることが可能になります。

1,000 以下で 1,000 と互いに素である数の個数が分かればそれが素数候補になります。

$1000=2^3\cdot5^3$　より，　$\varphi(1000)=1000\times\left(1-\dfrac{1}{2}\right)\left(1-\dfrac{1}{5}\right)=400$

ただ，これでは上限の個数 250 個をはるかに超えてしまいます。

そこで本文で述べたのと同じ方法で，1000 の前後で素因数の種類が多い数で調べてみます。

まず，1000 を超える数を調べましょう。

1001, 1002, 1003, …, 1049, 1050, 1051, 1053,

数 1050 は 2, 3, 5, 7 の倍数なので，候補の数になります。素因数分解すると，

$$1050=2\cdot3\cdot5^2\cdot7$$

これから，

$$\varphi(1050)=1050\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)=5\times1\times2\times4\times6=240$$

1050 と互いに素である 1050 以下の整数は 240 個であるため，1000 以下の素数は 250 以下ということがいえます。

次に，1000 未満の数を調べましょう。

$999, 998, \cdots, 992, 990$

数 990 が候補として浮かんできます。990 は，2, 3, 5, 11 の倍数になっています。素因数分解すると，

$$990 = 2 \cdot 3^2 \cdot 5 \cdot 11$$

オイラー関数の値を求めると，

$$\varphi(990) = 990 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{11}\right) = 3 \cdot 1 \cdot 2 \cdot 4 \cdot 10 = 240$$

240 個が素数候補になります。

これに 991 から 1000 までの 10 個の数を加えると，ちょうど 250 個になります。しかし，990 以下の 240 個には素数でない 1 も含まれています。だから，990 以下の素数候補は 241 個と考えると 1000 以下では 250 個を超えてしまいます。そこで，991 以上の偶数を除いた奇数 5 個を加えることで解決します。

では，その素数候補である奇数は本当に素数なのか調べてみましょう。

n 個の自然数にたいしてエラトステネスのふるいにかける最大素数は $\sqrt{n}$ 以下でしたが，この考え方は素数判定にも用いることができます。例えば 91 が素数であるかどうかは，$\sqrt{91} < 10$ より，9 以下の素数 2, 3, 5, 7 を調べるだけでいいのです。91 は明らかに 2, 3, 5 の倍数ではないので，7 の倍数か調べると，$91 = 7 \times 13$。よって 91 は素数ではありません。

991～1000 の奇数は 991，993，995，997，999 ですが, 993 と 999 は 3 の倍数, 995 は 5 の倍数なので, 素数候補は, 991 と 997 になります。，$\sqrt{1000} < 32$ なので，この 2 数を 31 以下の素数で割って調べると，どちらも素数であることが分かります。

以上より，1000 以下の素数候補は 243 個になりだいぶ絞り込むことができました。

ちなみに合同式を用いると簡単に倍数判定をすることができます。

3 の倍数は「各位の数の和か 3 の倍数」ですが，これは次の式から得られるものです。

$$10 \equiv 1 \pmod 3 \text{　より，} 10^n \equiv 1 \pmod 3$$

例えば 3 桁の数は,

$$100a + 10b + c \equiv a + b + c \pmod 3$$

11 の倍数も同様に,

$$10 \equiv -1 \pmod{11} \text{　より，} 10^2 \equiv 1 \pmod{11}$$

$$\therefore \quad 10^n \equiv \begin{cases} 1 & (n\text{は偶数}) \\ -1 & (n\text{は奇数}) \end{cases} \pmod{11}$$

これから，$100a + 10b + c \equiv a - b + c \pmod{11}$

7 と 13 の倍数は，本文でも触れましたが,

$$7 \times 11 \times 13 = 1001$$

であることを利用します（3 桁の数に 1001 を乗ずると，3 桁分上位にずらしてコピーされ，この性質を用いると，1 だけの数からなるレピュニット数の作り出すことができます。詳しいことは「不思議数との出会いの覚書」を参照)。

そこで，$p = 7, 11, 13$ とすると，

$$10^3 \equiv -1 \pmod p \text{　より，} 10^6 \equiv 1 \pmod p$$

$$\therefore \quad 10^{3n} \equiv \begin{cases} 1 & (n\text{は偶数}) \\ -1 & (n\text{は奇数}) \end{cases} \pmod p$$

これから，p (11 と 13 だけでなく 7 も含む)の倍数判定は，数を 3 桁ごとに区切り交互に和と差を繰り返し得られた数が p の倍数であればいいことになります。この操作により最終的には 3 桁以下の数になるので，あとは実際に p で割って調べます。ただそれも合同式を用いると割り算をしなくても次のように求めることはできます。

例えば 3 桁の 7 の倍数は，$10 = 7 \times 1 + 3$，$100 = 7 \times 14 + 2$ であることから,

$$100a + 10b + c \equiv 2a + 3b + c \pmod 7$$

12467 で調べると，

$$467 - 12 = 455 \;\Rightarrow\; 2 \times 4 + 5 \times 3 + 5 = 28 = 4 \times 7$$

これから 12467 は 7 の倍数であることが分かります。でも，このような操作を覚えることは必要でしょうか。

3 桁を 1 桁で割ることは暗算でそれほど難しいことではありません(この程度の暗算はできて欲しい)。ましてや電卓機能のある機器で思考をスルーして求めてしまうのはどうなのでしょうか。3 桁より桁数の多い数に対しては合同式の考え方を含めて理解しなければなりません。理解すべきことは原理でありそれから得られる僅少の結果ではないはずです。ある程度の道筋ができて結論に近づけたのなら後は直接数えるなど緩急自在に対応できることこそ大事なのではないでしょうか。

「1000 以下の素数の個数は 250 個以下を示せ」。この 1 行の問いから始めて今回は小手技にしては頁数の多い 12 ページのレポートを仕上げました。思考を巡らせ，道筋を判断し，解法を表現し，アイデアを膨らませていく。学習指導要領のねらいである「数学のよさ」は，このようなことではないのでしょうか。

(2021.3.15)