昔作ったファイルが見つかったので、掲載しておきましょう。少し間違っているかもしれません。その点はご了承ください。それでは、とても大切な定理を紹介します.

Theorem 1. 1 より大きなどんな自然数も，素因数分解が可能であり，素数の並べ方を考慮しなければ，結果はただ一つである.

少しむつかしいので証明は省略します．ただ，以下のことに気づくことはとても重要です．デタラメに挙げた 654852369741147785 52 という自然数を素因数分解しなさい，という問題があったとします．もしも上の定理がなければ，そもそも 654852369741147785 52 が素因数分解できるかわかりません．仮に，素因数分解できない場合は，問題として成立しないことに気づいてください．だって，素因数分解できないかもしれないのですから…．さらに，素因数分解の結果がただ一つでなければ，A さんと B さんの答えが異なっていても，どちらも丸という事にもなりうるでしょう．丸付けが大変．ところが，上の定理があるので，そう言った心配はいりません.

Definition 1. ある自然数の二乗であるような自然数を平方数という．例えば，$1^2, 2^2, 3^2, 4^2, 5^2$，つまり $1, 4, 9, 16, 25$ などは平方数である.

さて，次の問題を見てみましょう.

Problem 1. 120 にある自然数を掛けて，平方数にしたい．そのような自然数のうち最小の自然数はいくつか答えなさい.

上の問題のよくある解答例としては，以下のようなものでしょう.

Proof. 120 を素因数分解すると，$120 = 2^3 \cdot 3 \cdot 5$ である．よって，120 に 30 を掛ければ,

$$120 \cdot 30 = (2^3 \cdot 3 \cdot 5) \cdot (2 \cdot 3 \cdot 5) = 2^4 \cdot 3^2 \cdot 5^2 = (2^2 \cdot 3 \cdot 5)^2$$

となる．$2^2 \cdot 3 \cdot 5$ は自然数なので，$120 \cdot 30$ は平方数である．従って，求める自然数は 30 である． □

大抵の教科書や問題集には，このように書かれているでしょう．上の解答によれば，120 に 30 を掛けると平方数になるということでした．ところが，120 に 30 より小さい自然数を掛けても，絶対に平方数にならないことの説明はどこにもありません．つまり，30 がそのような”最小”の自然数であることは，何も説明していないのです．数学を良く知っている人は，そのような自然数のうち 30 が”最小”だと当たり前に思っています．当たり前だと思われることでも，説明できなければ，それは数学ではありません．もし答えを書いてあたっていても，それを説明できなければ，算数をしていると思われても，文句は言えないでしょう．それは，数学は非常に厳密であり，最も理想的な学問だからです．とは言え，30 がそのような自然数のなかで最小であることを説

明するのは，中学生には骨が折れるでしょう．だから，以下にその説明をします．訳分かんないやと思ったときは，飛ばしてください．もっと簡単に言える気がするのですが，どうしても説明が難しくなってしまいます．僕の実力不足ですね．

Lemma 2. どんな異なる n 個の素数 $p_1, p_2, ..., p_n$ についても，$\sqrt{p_1p_2...p_n}$ は有理数ではない．

Proof. 背理法を用いて証明する．異なる n 個のある素数 $p_1, p_2, ..., p_n$ について，$\sqrt{p_1p_2...p_n}$ は有理数だと仮定する．このとき，ある自然数 p, q を用いて

$$\sqrt{p_1p_2...p_n} = \frac{p}{q}$$

と書ける．両辺を 2 乗して q^2 を掛けると

$$p_1p_2...p_nq^2 = p^2$$

となる．$a := p^2 = p_1p_2...p_nq^2$ とおく．p, q は自然数なので，それぞれの素因数分解を考える．まず p について，すべて異なる素数 $\alpha_1, \alpha_2, ..., \alpha_l$ と自然数 $r_1, r_2, ..., r_l$ を用いて

$$p = {\alpha_1}^{r_1}{\alpha_2}^{r_2}...{\alpha_l}^{r_l}$$

と素因数分解できたとする．q について，すべて異なる素数 $\beta_1, \beta_2, ..., \beta_m$ と自然数 $s_1, s_2, ..., s_m$ を用いて

$$q = {\beta_1}^{s_1}{\beta_2}^{s_2}...{\beta_m}^{s_m}$$

と素因数分解できたとする．このとき，$p^2 = p_1p_2...p_nq^2$ より，

$$\begin{aligned}
{\alpha_1}^{2r_1}{\alpha_2}^{2r_2}...{\alpha_l}^{2r_l} &= ({\alpha_1}^{r_1}{\alpha_2}^{r_2}...{\alpha_l}^{r_l})^2 \\
&= p^2 \\
&= a \\
&= p_1p_2...p_nq^2 \\
&= (p_1p_2...p_n)({\beta_1}^{s_1}{\beta_2}^{s_2}...{\beta_m}^{s_m})^2 \\
&= (p_1p_2...p_n){\beta_1}^{2s_1}{\beta_2}^{2s_2}...{\beta_m}^{2s_m}
\end{aligned}$$

である．上式の左辺は，素数の偶数乗らの積である．一方，上式の右辺は，素数の奇数乗の積も現れている．従って，自然数 a は，二通りの素因数分解が存在することになる．これは Theorem 1 に矛盾．ゆえに，どんな異なる n 個の素数 $p_1, p_2, ..., p_n$ についても，$\sqrt{p_1p_2...p_n}$ は有理数ではない． □

上の補題 (Lemma 2) を用いると，以下の定理 (Theorem 3) が得られます．

Theorem 3. 1より大きなどんな自然数nについても，以下が成り立つ．nは，すべて異なる素数$p_1, p_2, ..., p_m$と自然数$q_1, q_2, ..., q_m$を用いて，

$$n = {p_1}^{q_1}{p_2}^{q_2}...{p_m}^{q_m}$$

と因数分解できたとする．このとき，一般性を失うことなく，

$$q_1, q_2, ..., q_l : \text{奇数}, \quad q_{l+1}, q_{l+2}, ..., q_m : \text{偶数}$$

としてもよい．nに自然数aを掛けて，naが平方数になるには，aは$p_1p_2...p_l$の倍数でなければいけない．特に，naが平方数になるような最小の自然数aは$p_1p_2...p_l$である．

Proof. 定理の仮定より

$$q_1,\ q_2,\ ...,\ q_l : \text{奇数}, \quad q_{l+1},\ q_{l+2},\ ...,\ q_m : \text{偶数}$$

だったので，ある自然数$s_1, s_2, ..., s_m$を用いて

$$q_1 = 2s_1 - 1, \quad q_2 = 2s_2 - 1, \quad ..., \quad q_l = 2s_l - 1,$$

$$q_{l+1} = 2s_{l+1}, \quad q_{l+2} = 2s_{l+2}, \quad ..., \quad q_m = 2s_m,$$

と書ける．自然数aを素因数分解する．すべて異なる素数$\alpha_1, \alpha_2, ..., \alpha_k$と自然数$r_1, r_2, ..., r_k$を用いて，

$$a = {\alpha_1}^{r_1}{\alpha_2}^{r_2}...{\alpha_k}^{r_k}$$

と素因数分解できたとする．一般性を失うことなく，

$$r_1, r_2, ..., r_j : \text{奇数}, \quad r_{j+1}, r_{j+2}, ..., r_k : \text{偶数}$$

としてもよい．よって，ある自然数$t_1, t_2, ..., t_k$を用いて

$$r_1 = 2t_1 - 1, \quad r_2 = 2t_2 - 1, \quad ..., \quad r_j = 2t_j - 1,$$

$$r_{j+1} = 2t_{j+1}, \quad r_{j+2} = 2t_{j+2}, \quad ..., \quad r_k = 2t_k,$$

と書ける．このとき

$$\begin{aligned}
& na \\
= \ & ({p_1}^{q_1}{p_2}^{q_2}...{p_m}^{q_m})({\alpha_1}^{r_1}{\alpha_2}^{r_2}...{\alpha_k}^{r_k}) \\
= \ & ({p_1}^{q_1}{p_2}^{q_2}...{p_l}^{q_l})({\alpha_1}^{r_1}{\alpha_2}^{r_2}...{\alpha_j}^{r_j}) \\
& ({p_{l+1}}^{q_{l+1}}{p_{l+2}}^{q_{l+2}}...{p_m}^{q_m})({\alpha_{j+1}}^{r_{j+1}}{\alpha_{j+2}}^{r_{j+2}}...{\alpha_k}^{r_k}) \\
= \ & ({p_1}^{2s_1-1}{p_2}^{2s_2-1}...{p_l}^{2s_l-1})({\alpha_1}^{2t_1-1}{\alpha_2}^{2t_2-1}...{\alpha_j}^{2t_j-1}) \\
& ({p_{l+1}}^{2s_{l+1}}{p_{l+2}}^{2s_{l+2}}...{p_m}^{2s_m})({\alpha_{j+1}}^{2t_{j+1}}{\alpha_{j+2}}^{2t_{j+2}}...{\alpha_k}^{2t_k}) \\
= \ & (p_1p_2...p_l)(\alpha_1\alpha_2...\alpha_j) \\
& ({p_1}^{2s_1-2}{p_2}^{2s_2-2}...{p_l}^{2s_l-2})({\alpha_1}^{2t_1-2}{\alpha_2}^{2t_2-2}...{\alpha_j}^{2t_j-2}) \\
& ({p_{l+1}}^{2s_{l+1}}{p_{l+2}}^{2s_{l+2}}...{p_m}^{2s_m})({\alpha_{j+1}}^{2t_{j+1}}{\alpha_{j+2}}^{2t_{j+2}}...{\alpha_k}^{2t_k})
\end{aligned}$$

と計算できる．よって，

$$\begin{array}{rc} & \sqrt{na} \\ = & \sqrt{(p_1p_2...p_l)(\alpha_1\alpha_2...\alpha_j)} \\ & ({p_1}^{s_1-1}{p_2}^{s_2-1}...{p_l}^{s_l-1})({\alpha_1}^{t_1-1}{\alpha_2}^{t_2-1}...{\alpha_j}^{t_j-1}) \\ & ({p_{l+1}}^{s_{l+1}}{p_{l+2}}^{s_{l+2}}...{p_m}^{s_m})({\alpha_{j+1}}^{t_{j+1}}{\alpha_{j+2}}^{t_{j+2}}...{\alpha_k}^{t_k}) \quad ... \quad (*) \end{array}$$

である．na は平方数なので，$\sqrt{na}$ は自然数である．今，

$$M := \sqrt{(p_1p_2...p_l)(\alpha_1\alpha_2...\alpha_j)}$$

とおき，これに注目する．もし $p_1, p_2, ..., p_l, \alpha_1, \alpha_2, ..., \alpha_j$ がすべて異なれば，Lemma 2 より，M は有理数ではない．しかし，これは式 (*) に矛盾．従って，一般性を失うことなく，$\alpha_1, ..., \alpha_j$ の中に p_1 と等しいものがあるとしてもよい．さらに一般性を失うことなく，$\alpha_1 = p_1$ としてもよい．しからば，

$$M = p_1\sqrt{(p_2...p_l)(\alpha_2...\alpha_j)}$$

となる．もし $p_2, ..., p_l, \alpha_2, ..., \alpha_j$ がすべて異なれば，Lemma 2 より，$\frac{M}{p_1}$ は有理数ではない．しかし，これは式 (*) に矛盾．従って，一般性を失うことなく，$\alpha_2, ..., \alpha_j$ の中に p_2 と等しいものがあるとしてもよい．さらに一般性を失うことなく，$\alpha_2 = p_2$ としてもよい．しからば，

$$M = p_1p_2\sqrt{(p_3...p_l)(\alpha_3...\alpha_j)}$$

となる．この操作を有限回繰り返せば，結局，

$$l = j,\ p_1 = \alpha_1,\ ...,\ p_l = \alpha_l$$

が得られる．これは，自然数 a が $p_1p_2...p_l$ の倍数であることを示唆する．ところで，$np_1p_2...p_l$ が平方数であることは明らかである．ゆえに，na が平方数になるような最小の自然数 a は $p_1p_2...p_l$ であることも直ちにわかる．この Theorem の証明は，たった今完了した． □

とても難しくやっているような気がしますが，一般的に述べているので，そうとも言えないかもしれません．なにはともあれ，Problem 1 のような問題にぶちあたったら，「野川さんが変な証明をしたから，大丈夫だ」と思いながら，まずは素因数分解をして，指数が偶数になるように足りない素数を最小限に補えば，答えになります．安心して問題を解いてください．