1.（1） 整数 a と正の整数 b に対し，a を b で割ったときの「商」と「余り」の定義をそれぞれ述べなさい．また，その定義に基づいて，-1 を 2021 で割ったときの商と余りを求めなさい．

（2） a, b, c は整数とし，a と b のうち少なくとも一方は 0 でないものとします．a, b, c に関する次の条件（i），（ii），（iii）について，（ii）は（i）であるための必要十分条件であることを示しなさい．さらに，（iii）は（i）であるための必要十分条件であるかどうかを調べなさい．

（i） $ax+by=c$ をみたす整数 x，y が存在する．

（ii） p が素数で n が正の整数ならば，

$ax+by+p^nz=c$

をみたす整数 x，y，z が存在する．

（iii） p が素数ならば，

$ax+by+pz=c$

をみたす整数 x，y，z が存在する．

（21　鳴門教育大・教育）

《整数の命題の証明（D40）》

2.（1） 整数 a と正の整数 b に対し，a を b で割ったときの「商」と「余り」の定義をそれぞれ述べなさい．また，その定義に基づいて，-1 を 2021 で割ったときの商と余りを求めなさい．

（2） a, b, c は整数とし，a と b のうち少なくとも一方は 0 でないものとします．a, b, c に関する次の条件（i），（ii），（iii）について，（ii）は（i）であるための必要十分条件であることを示しなさい．さらに，（iii）は（i）であるための必要十分条件であるかどうかを調べなさい．

（i） $ax+by=c$ をみたす整数 x，y が存在する．

（ii） p が素数で n が正の整数ならば，

$ax+by+p^nz=c$

をみたす整数 x，y，z が存在する．

（iii） p が素数ならば，

$ax+by+pz=c$

をみたす整数 x，y，z が存在する．

（21　鳴門教育大・教育）

考え方 （2） 題意の解釈が難しい．入試問題は「変数と定数」の区別を書かないものであるが，そのために正しく題意を取れない危険性が高い．（ii）は「どのような素数 p，どのような正の整数 n に対しても，題意の等式が成り立つような整数 x, y, z が存在する」ということであるが，「存在」という表現は高校では出てこないために，生徒は「なんでもいいからあればいいのでしょ？$z=0$ にしたら皆同じ式だ．$z=0$ がある．」と無茶苦茶をする．a, b, c は定数で，動かせない．解答者が考察に関して選択権があるのは p, n であり，z は，ひとまずは，勝手に決めてよいものではない．

▶解答◀ （1） すべての b の整数倍

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

を並べると，a は，どれかに一致するかどれかの間に入る．すなわち，ある整数 q が存在して $bq \leqq a < b(q+1)$ となる．このとき $0 \leqq a-bq < b$ であるから $a-bq=r$ として

$$a=bq+r,\ 0 \leqq r < b$$

となる．このとき，整数 q，r がそれぞれ，a を b で割ったときの「商」と「余り」である．

$a=-1$，$b=2021$ のとき

$$-1=2021\cdot(-1)+2020$$

で，2020 は $0 \leqq 2020 < 2021$ を満たすから，

求める商は **-1**，余りは **2020** である．

（2） 下の ① で最大公約数が出てくる．0 や負の整数を含む最大公約数は高校の範囲外であり，問題文は「答案を書きやすくする配慮」に欠ける．a, b の最大公約数を g とする．ここでは g を次のように定義する．

$ab \neq 0$ のとき，$|a|, |b|$ の最大公約数を g とする．

$a=0$ のときは $a=0\cdot b$ として $|b|$ を g とする．たとえば $a=0, b=-4$ のとき a, b は素因数 2 を 2 個もつと考え，$g=4$ とする．

$b=0$ のときは $b=0\cdot a$ として $|a|$ を g とする．

このとき $ax+by$ は g の倍数であり

（i）$\Longleftrightarrow$ c が g の倍数 ……①

は有名である．答案本体を短くするためこれを既知とする．注で補う．

（ii）について：「任意の素数 p，および任意の自然数 n に対して $ax+by+p^nz=c$ をみたす整数 x，y，z が存在する」

ならば，a，b が共通にもつ素因数があれば，それを p とし，a, b がもつ p の個数の小さい方（等しいときはその値）を n とすると，$ax+by+p^n z=c$ の左辺は p^n の倍数になる．よって c は p^n の倍数である．これが a, b の共通のすべての素因数 p について言えるから c は g の倍数になる．逆に c が g の倍数ならば，$z=0$ として $ax+by=c$ となる整数 x, y が存在するから，

（ⅰ）$\Longleftrightarrow$（ⅱ）……②

である．

a, b が共通にもつ素因数がなければ $g=1$ で①，②は成り立つ．

（ⅱ）は（ⅰ）であるための必要十分条件である．

ここで，記号を導入する．自然数 n に対して，n の互いに異なる素因数の積を n の根基と呼び，$\mathrm{rad}(n)$ と書く．① の類似物として

（ⅲ）$\Longleftrightarrow$ c が $\mathrm{rad}(g)$ の倍数 ……（＊）

であることを示す．これを認めれば，（ⅰ）$\Longrightarrow$（ⅲ）はすぐにわかる．また，（ⅲ）$\Longrightarrow$（ⅰ）の反例も構成できる．

例えば，$(a, b, c)=(4, 12, 2)$ のとき $g=4$ である．c は $\mathrm{rad}(g)=\mathrm{rad}(4)=2$ の倍数であるから，（ⅲ）は成立しているが，c は 4 の倍数ではないから（ⅰ）は成立しない．よって，**（ⅲ）は（ⅰ）であるための必要条件であるが，十分条件ではない．**

さて，（＊）を示そう．

（$\Longrightarrow$） a, b が共通にもつ素因数があれば，それを p とする．このとき，$ax+by+pz=c$ の左辺は p の倍数になる．よって c は p の倍数である．これが a, b の共通のすべての素因数 p について言えるから c は $\mathrm{rad}(g)$ の倍数になる．

（$\Longleftarrow$） ① より，任意の素数 p に対して，（適切な z を取ることによって）$c-pz$ を g の倍数にすることができれば，（ⅲ）が言えたことになる．

ここで，任意の素数 p に対して，g と p の最大公約数は $\mathrm{rad}(g)$ の約数であることから，c が $\mathrm{rad}(g)$ の倍数，特に g と p の最大公約数の倍数であることを合わせると，① より，

$$gk+pz=c$$

となる整数 k, z が存在する．すなわち，任意の素数 p に対して，$c-pz$ を g の倍数にすることができることが言えたから，（ⅲ）が示された．

注意 1°【① について】

g は解答に書いた意味での a, b の最大公約数である．

（a） $b>0, g\neq 1$ のとき．

$c-a\cdot 0, c-a\cdot 1, \cdots, c-a\cdot(b-1)$ ……③

は b 個の整数である．これらを b で割った余りが全部異なれば，0 から $b-1$ が 1 個ずつ現れ，③ の中に b の倍数のものがあるから $c-ax=by$ となる整数 x, y が存在する．

③ を b で割った余りの中に等しいものがあると仮定すると $0\leqq i<j\leqq b-1$ となる整数 i, j で

$(c-ai)-(c-aj)=a(j-i)$

が b の倍数になるものがあるが，$0<j-i<b$ であり，a と b は互いに素であるから矛盾する．ゆえにそのようなものはない．

（b） $b<0$ のとき．$by=(-b)(-y)$ であるから $-b$ を新たな b だと思って上と同様に考えればよい．

（c） $b=0$ のとき．$ax+by=c$ は $ax=c$ となり，c は g の倍数である．

（d） a, b が互いに素でないとき，$ax+by$ は g の倍数であるから，

$a=ga', b=gb', c=gc'$ として，$ax+by=c$ の両辺を g で割った式は $a'x+b'y=c'$ となる．これを満たす整数 x, y が存在することは以上で示されている．

なお，ユークリッドの互除法の応用として $ax+by=c$ の特殊解を見つける解法もある．この解法をとる場合，a, b は正でなければならないから，出題者の負や 0 を許した出題姿勢はよくない．無駄に面倒である．

2°【p, n は都合の良いものだけを考えるのではない】

上の解答で p を a, b の共通因数，n を a, b がもつ個数の小さい方の指数にとっているが，「どのような p, n に対してもこうなっている」というのであるから，p が a, b がもっていない素数であったり，n が小さい自然数のときには $ax+by=c, z=0$ になるという形である．